FDA CENTER FOR DEVICES &
RADIOLOGICAL HEALTH (CDRH),
NATIONAL HEALTH INFORMATION SHARING
ANALYSIS CENTER (NH-ISAC),
THE DEPARTMENT OF HEALTH AND
HUMAN SERVICES (HHS), AND
THE DEPARTMENT OF HOMELAND SECURITY (DHS)
PRESENT A PUBLIC WORKSHOP:

Moving Forward: Collaborative Approaches to Medical Device Cybersecurity

January 20-21, 2016

FDA White Oak Campus

Silver Spring, MD

WELCOME

January 20, 2016

Dear Colleagues,

On behalf of the FDA and its co-sponsors – the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the Department of Health and Human Services (HHS) Critical Infrastructure Protection Program, and the National Healthcare Information Sharing and Analysis Center (NH-ISAC) –, it is with great enthusiasm that I welcome you to our public workshop, ***'Moving Forward: Collaborative Approaches to Medical Device Cybersecurity.'***

Our objective is to highlight past collaborative efforts, increase awareness of existing maturity models (i.e. frameworks leveraged for benchmarking an organization's processes) which are used to evaluate cybersecurity status, standards, and tools in development, and to engage the multi-stakeholder community in focused discussions on unresolved gaps and challenges that have hampered progress in advancing medical device cybersecurity.

Safeguarding the nation's public health with respect to medical device cybersecurity requires attentiveness to the total product life cycle, from design to obsolescence. We believe that progress in this space will emerge through efforts that bring together the "whole of community". We see this public workshop as an opportunity to engage diverse stakeholders across the medical device ecosystem in critical conversations about key topic areas such as cyber hygiene, information sharing, coordinated vulnerability disclosure and management, and the adaptation of the Common Vulnerability Scoring System (CVSS) and/or other cybersecurity risk assessment tools for the medical device operational environment. In convening this interactive public meeting, we aim to gain implementation-level insights that would ultimately enable the sector to readily share threat and vulnerability information, enhance stakeholder collaborations, better understand and, most importantly, cultivate a culture that will proactively address medical device vulnerabilities before there is an impact on patient care and safety.

We express overwhelming appreciation to all of you who have made this public meeting possible. Much gratitude goes to our workshop partners – DHS, HHS, and the NH-ISAC – and FDA's Center for Devices and Radiological Health (CDRH) Cybersecurity Working Group, the Emergency Preparedness/Operations & Medical Countermeasures (EMCM) Program, the Office of Communications and Education staff, the Center Science Council staff, and the Digital Communication Media staff. Planning, organizing and executing a meeting of this size and magnitude is a massive undertaking and today's meeting would not have occurred without their extraordinary efforts. We would also like to recognize our speakers, moderators, panelists, and facilitators for taking time out of their hectic schedules and coming from near and far to partner with us in strengthening cybersecurity within healthcare and public health (HPH).

As medical device cybersecurity continues to evolve, we have witnessed great passion and commitment from so many of you. Your dedication to the field, your shared insights, and subject matter expertise are key ingredients and we look forward to your ongoing participation. We may approach cyber security from different vantage points, but we all have one common goal and that is to protect patients. Engaging in collaborative activities, as we are doing today, enables us to strike the right balance of delivering the best care to patients that medical device technologies can offer today while promoting the safety and necessary security of these devices.

Sincerely,
Suzanne B. Schwartz, MD, MBA

FDA Disclaimer

The views expressed in this Public Workshop are those of the authors and do not necessarily reflect the official policy or position of the U.S. Food and Drug Administration, the Department of Health and Human Services, or the United States Government, and should not be used for advertising or product endorsement purposes. Reference to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its approval, endorsement, recommendation, or favoring by the United States Government or any department, agency, office, or branch thereof.

Contents

Agenda at a Glance

Day 1: January 20, 2016	
Time	**Topic**
8:30am-9:00am	Registration (for pre-registered attendees)
9:00am-9:05am	Welcome Remarks – Stephen Ostroff, MD
9:05am-9:15am	Medical Device Cybersecurity: A Year in Reflection and Looking Ahead
9:15am-10:00am	Session I Plenary Panel: Cyber Threat Landscape within the Healthcare and Public Health Sector
10:00am-11:30am	Session II Plenary Panel: FDA's Current Thinking: Implementation of the NIST "Framework for Improving Critical Infrastructure Cybersecurity“ for Strengthening Security throughout the Total Product Life Cycle
11:30am-11:40am	**BREAK**
11:40am-12:40pm	Information Sharing and Analysis Organization (ISAO) Breakout Session
12:40pm-1:40pm	**LUNCH**
1:40pm-2:55pm	Session III Plenary Panel: Key Ingredients for Effective Postmarket Management of Medical Device Vulnerabilities - Vulnerability Handling Processes and Coordinated Vulnerability Disclosure
2:55pm-3:05pm	**BREAK**
3:05pm-3:55pm	Coordinated Vulnerability Disclosure Breakout Session
3:55pm-4:05pm	**Return from Breakout**
4:05pm-5:20pm	Session IV Plenary Panel: Overcoming Challenges Manufacturers Face with Increased Cybersecurity Collaboration
5:20pm-5:35pm	ISAO Breakout Report Out, Adjourn
Day 2: January 21, 2016	
8:30am-9:00am	Registration (for pre-registered attendees)
9:00am-9:35am	Welcome, Coordinated Vulnerability Disclosure Breakout Report Out, Recap Day 1
9:35am-9:55am	Keynote Address: Marty Edwards, Director of ICS-CERT
9:55am-10:55am	Session V Plenary Panel: Identifying and Crafting Action Plans to Address Gaps and Challenges in Strengthening the Cybersecurity Stance of the Medical Device Ecosystem
10:55am-11:05am	**BREAK**
11:05am-12:15pm	Gaps & Action Plan Break Out Session
12:15pm-1:15pm	**LUNCH**
1:15pm-2:15pm	Session VI Plenary Panel: Gaining Situational Awareness of Current Activities in the Healthcare and Public Health Sector to Enhance Medical Device Cybersecurity
2:15pm-3:15pm	Session VII Plenary Panel: Risk Assessment Tools for the Medical Device Operational Environment
3:15pm-3:25pm	**BREAK**
3:25pm-4:25pm	Session VIII Plenary Panel: Adapting and/or Implementing Medical Device Cybersecurity Standards
4:25pm-5:30pm	Gaps & Action Plan Breakout Report Outs, Workshop Recap, and Closing Remarks

Agenda Day 1: January 20, 2016

Time	Topic	
8:00am-9:00am	Registration (for pre-registered attendees)	
9:00am-9:05am	**Welcome Remarks**	Stephen Ostroff, MD Commissioner (Acting), Food and Drug Administration
9:05am-9:15am	**Medical Device Cybersecurity: A Year in Reflection and Looking Ahead**	Suzanne Schwartz, MD, MBA Associate Director for Science and Strategic Partnerships, Acting Director Emergency Preparedness/Operations and Medical Countermeasures Program (EMCM), Center for Devices and Radiological Health (CDRH) Food and Drug Administration (FDA)
9:15am-10:00am	**Session I Plenary Panel: Cyber Threat Landscape within the Healthcare and Public Health Sector**	**Panel Moderator:** Stephen Curren, MS – Director, Division of Resilience and Infrastructure Coordination, Office of Emergency Management (OEM) / Assistant Secretary for Preparedness and Response (ASPR) / HHS **Discussants:** • Denise Anderson, MBA – Executive Director, National Healthcare Information Sharing and Analysis Center (NH-ISAC) • Scott Erven – Associate Director, Protiviti • Rick Hampton – Wireless Communications Manager, Partners HealthCare System • Kevin Hemsley – Project Manager, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) / Department of Homeland Security (DHS) • Michael McNeil, MBA – Global Product Security and Services Officer, Philips Healthcare • Kevin McDonald, BSN, ME-PD, CISSP – Director of Clinical Information Security, Mayo Clinic • Jeffrey Vinson – Vice President & Chief Information Security Officer, Information Security Department,

		Harris Health System
10:00am-11:30am	**Session II Plenary Panel: FDA's Current Thinking: Implementation of the NIST "Framework for Improving Critical Infrastructure Cybersecurity“ for Strengthening Security throughout the Total Product Life Cycle**	**Panel Moderator:** Linda Ricci – Biomedical Engineer, Office of Device Evaluation (ODE) / CDRH / FDA **Discussants:** • Denise Anderson, MBA – Executive Director, NH-ISAC • Seth Carmody, PhD – Device Reviewer, Office of In Vitro Diagnostics and Radiological Health (OIR) / FDA • Josh Corman – Founder I Am The Cavalry & Chief Technology Officer Sonatype • Kevin Fu, PhD – Chief Scientist Virta Labs & Director Archimedes Center for Medical Device Security, University of Michigan • Elisabeth George, MS – Vice President of Global Regulation & Standards Philips Healthcare • Kevin Hemsley – ICS-CERT / DHS • Patrick Kehoe, MBA – Chief Marketing Officer, Arxan • Ron Mehring, MBA, CISSP – Vice President Technology & Security, Texas Health Resources • Colin Morgan, CISSP, GPEN – Head of Global Product Security, Information Security & Risk Management, Johnson & Johnson • John Murray, MS – Expert Regulatory Review Scientist, Office of Compliance (OC) / CDRH /FDA • Henri “Rik” Primo, MS – Director Strategic Relationships, Digital Health Services, Siemens Healthcare & Medical Imaging and Technology Alliance (MITA) • Zach Rothstein, JD – Associate Vice President, Technology & Regulatory Affairs, AdvaMed • Suzanne Schwartz, MD, MBA – Office of the Center Director (OCD) / CDRH / FDA • Ryan Winn – Director, Information Systems, Munson Healthcare

		• Axel Wirth, CPHIMS, CISSP, HCISPP – Distinguished Technical Architect, Public Sector/Healthcare, Symantec Corp
11:30am-11:40am	**BREAK**	
11:40am-12:40am	**Information Sharing and Analysis Organization (ISAO) Breakout Session**	
12:40am-1:40pm	**LUNCH**	
1:40pm-2:55pm	**Session III Plenary Panel: Key Ingredients for Effective Postmarket Management of Medical Device Vulnerabilities - Vulnerability Handling Processes and Coordinated Vulnerability Disclosure**	**Panel Moderator:** Steve Christey Coley – Principal INFOSEC Engineer, Cybersecurity Division, The MITRE Corporation **Discussants:** • Scot Copeland BSITSec, Sec+, MCP – Medical I.T. Network Risk Manager, Scripps Health • Allan Friedman, PhD – Director of Cybersecurity, National Telecommunications and Information Administration (NTIA) / Department of Commerce • Kevin Hemsley – ICS-CERT / DHS • Art Manion – Senior Vulnerability Analyst, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University • Michael McNeil, MBA – Global Product Security and Services, Philips Healthcare • Hannes Molsen, M.Sc. – Product Security Manager, Draeger & I Am The Cavalry • Katie Moussouris – Chief Policy Officer, HackerOne • Billy Rios, MBA, MSIS, CISSP – Founder, WhiteScope LLC • Suzanne Schwartz, MD, MBA – OCD / CDRH / FDA • Beau Woods – I Am The Cavalry
2:55pm-3:05pm	**BREAK**	
3:05pm-3:55pm	**Coordinated Vulnerability Disclosure Breakout**	

	Session	
3:55pm-4:05pm	**Return from Breakout**	
4:05pm-5:20pm	**Session IV Plenary Panel: Overcoming Challenges Manufacturers Face with Increased Cybersecurity Collaboration**	**Panel Moderator:** Zach Rothstein, JD – Associate Vice President, Technology & Regulatory Affairs, AdvaMed **Discussants**: • Steve Abrahamson, BSME, MBA – Director, Product Security Programs, GE Healthcare • Bill Aerts, CISSP, CISM – Director Product Security, Global Privacy and Security Office, Medtronic • Carl Anderson, JD – Vice President, Government Affairs, Health Information Trust Alliance (HITRUST) • Scot Copeland BSITSec, Sec+, MCP – Scripps Health • Allan Friedman, PhD – NTIA / Department of Commerce • Harley Geiger, JD, MA, CIPP/US – Director of Public Policy, Rapid7 • Ralph Hall, JD – Partner Leavitt Partners & Professor of Practice University of Minnesota • Kevin Hemsley – ICS-CERT / DHS • Marie Moe, PhD – Research Scientist, Department of Software Engineering, Safety and Security, SINTEF ICT • Hannes Molsen, M.Sc. – Draeger & I Am The Cavalry • Katie Moussouris – HackerOne • Dale Nordenberg, MD – Executive Director Medical Device Innovation, Safety, and Security Consortium (MDISS) & CEO Novasano Health and Science • Bakul Patel, MS – Associate Director for Digital Health, OCD / CDRH / FDA • Billy Rios, MBA, MSIS, CISSP – WhiteScope LLC • Beau Woods – I Am The Cavalry
5:20pm-5:35pm	**ISAO Breakout Report Out, Adjourn**	Principal Facilitators Suzanne Schwartz, MD, MBA Associate Director for Science and

		Strategic Partnerships, Acting Director Emergency Preparedness/Operations and Medical Countermeasures Program (EMCM), Center for Devices and Radiological Health (CDRH) Food and Drug Administration (FDA)

Agenda Day 2: January 21, 2016

8:30am-9:00am	**Registration (for pre-registered attendees)**	
9:00am-9:35am	**Welcome, Coordinated Vulnerability Disclosure Breakout Report Out, Recap Day 1**	Suzanne Schwartz, MD, MBA Associate Director for Science and Strategic Partnerships, Acting Director Emergency Preparedness/Operations and Medical Countermeasures Program (EMCM), Center for Devices and Radiological Health (CDRH) Food and Drug Administration (FDA)
9:35am-9:55am	**Keynote Address**	Marty Edwards Director Industrial Control Systems Cyber Emergency Response Team, National Cybersecurity and Communications Integration Center (NCCIC), Office of Cybersecurity and Communications (CS&C), Department of Homeland Security
9:55am-10:55am	**Session V Plenary Panel: Identifying and Crafting Action Plans to Address Gaps and Challenges in Strengthening the Cybersecurity Stance of the Medical Device Ecosystem**	**Panel Moderator:** Margie Zuk, MS – Senior Principal Cybersecurity Engineer, The MITRE Corporation **Discussants:** • Scott Erven – Protiviti • Ben Flatgard, MA – National Security Council, White House • Jim Jacobson – Chief Product and Solution Security Officer, Siemens Healthcare • Marie Moe, PhD – Department of Software Engineering, Safety and Security, SINTEF ICT • Iliana Peters, J.D., LL.M – Senior Advisor for HIPAA Compliance and Enforcement, Office of Civil Rights (OCR) • Linda Ricci – ODE / CDRH / FDA • Lucia Savage, JD – Chief Privacy Officer, Office of the National Coordinator for Health Information Technology (ONC) • Roberto Suarez, HCISPP – Product Security Manager, Becton Dickinson • Jeffrey Vinson – Information Security Department, Harris

		Health System - Ryan Winn – Information Systems, Munson Healthcare
10:55am-11:05am	**BREAK**	
11:05am-12:15pm	**Gaps & Action Plan Break Out Session**	
12:15pm-1:15pm	**LUNCH**	
1:15pm-2:15pm	**Session VI Plenary Panel: Gaining Situational Awareness of Current Activities in the Healthcare and Public Health Sector to Enhance Medical Device Cybersecurity**	**Panel Moderator:** Stephen Curren, MS – Office of Emergency Management (OEM) / Assistant Secretary for Preparedness and Response (ASPR) / HHS **Discussants:** - Denise Anderson, MBA – NH-ISAC - Josh Corman – I am The Cavalry & Sonatype - Bryan Cline, PhD – Vice President, Standards & Analytics, HITRUST - Kevin Fu, PhD – Virta Labs & Archimedes Center for Medical Device Security, University of Michigan - Julian Goldman, MD – Medical Director of Biomedical Engineering Partners HealthCare & Director Medical Device Interoperability Program - Ralph Hall, JD – Leavitt Partners & University of Minnesota - Lee Kim, BS, JD – Director of Privacy and Security, Healthcare Information and Management Systems Society (HIMSS) - Deborah Kobza, CGEIT, JIEM – President/CEO, The Global Institute for Cybersecurity + Research (GICSR) - Marie Moe, PhD – Department of Software Engineering, Safety and Security, SINTEF ICT - Gavin O’Brien, MS – Computer Scientist, National Cybersecurity Center of Excellence (NCCoE), National Institute of Standards and Technology (NIST) - Dale Nordenberg, MD – MDISS &

		Novasano Health and Science
2:15pm-3:15pm	**Session VII Plenary Panel: Risk Assessment Tools for the Medical Device Operational Environment**	**Panel Moderator:** Marty Edwards, Director Industrial Control Systems Cyber Emergency Response Team, National Cybersecurity and Communications Integration Center (NCCIC), Office of Cybersecurity and Communications (CS&C), Department of Homeland Security **Discussants:** • Harold Booth – Computer Scientist, Computer Security Division (CSD) / Information Technology Laboratory (ITL), NIST • Penny Chase, MS, MA – Information Technology and Cybersecurity Integrator, The MITRE Corporation • Seth Carmody, PhD – OIR / FDA • Scott Erven – Protiviti • Rick Hampton – Partners HealthCare System • Dan Lyon – Principal Consultant, Cigital, Inc • Michael Murray – Director of Product Development Security, GE Healthcare • Henri “Rik” Primo, MS – Digital Health Services, Siemens Healthcare & MITA • Billy Rios, MBA, MSIS, CISSP – WhiteScope LLC • Roberto Suarez, HCISPP – Becton Dickinson • Axel Wirth, CPHIMS, CISSP, HCISPP – Public Sector/Healthcare, Symantec Corp
3:15pm-3:25pm	**BREAK**	
3:25pm-4:25pm	**Session VIII Plenary Panel: Adapting and/or Implementing Medical Device Cybersecurity Standards**	**Panel Moderator:** Ken Hoyme, MS – Distinguished Scientist, Adventium Labs & Association for the Advancement of Medical Instrumentation (AAMI) **Discussants:** • Brian Fitzgerald, B.Sc – Senior Technical Manager HPC and Cybersecurity, Office of Science and Engineering Laboratories

		(OSEL) / CDRH / FDA - Anura Fernando, MS – Principal Engineer for Medical Software & Systems Interoperability, Underwriters Laboratories - Kevin Fu, PhD – Virta Labs & Archimedes Center for Medical Device Security, University of Michigan - Michelle Jump, MS – Principal Regulatory Affairs Specialist, Stryker Connected Care, Stryker Corporation - David Klonoff, M.D., FACP, FRCP (Edin), Fellow AIMBE – Medical Director, Diabetes Research Institute, Mills-Peninsula Health Services - Kevin McDonald, BSN, ME-PD, CISSP – Mayo Clinic - Michael McNeil, MBA – Global Product Security and Services, Philips Healthcare - Katie Moussouris – HackerOne - Gavin O'Brien, MS – NCCoE / NIST - Chana O'Leary, BSN, MA – Senior Security Consultant, TÜV Rheinland-OpenSky Corporation
4:25pm-5:30pm	**Gaps & Action Plan Breakout Report Outs, Workshop Recap, and Closing Remarks**	Suzanne Schwartz, MD, MBA Associate Director for Science and Strategic Partnerships, Acting Director Emergency Preparedness/Operations and Medical Countermeasures Program (EMCM), Center for Devices and Radiological Health (CDRH) Food and Drug Administration (FDA)

Cybersecurity Public Workshop Session Descriptions, Objectives, and Questions for Consideration

Day 1

Welcome Remarks (9:00am-9:05am)

Stephen Ostroff, MD

Commissioner (Acting), Food and Drug Administration

Medical Device Cybersecurity: A Year in Reflection and Looking Ahead (9:05am-9:15am)

Suzanne Schwartz, MD, MBA

Associate Director for Science and Strategic Partnerships, Acting Director Emergency Preparedness/Operations and Medical Countermeasures Program (EMCM), Center for Devices and Radiological Health (CDRH) Food and Drug Administration (FDA)

Session I Plenary Panel (9:15am-10:00am) **– Cyber Threat Landscape within the Healthcare and Public Health Sector**

Moderator: Stephen Curren, MS – Office of Emergency Management (OEM) / Assistant Secretary for Preparedness and Response (ASPR) / HHS

Session Discussants:

Denise Anderson, MBA – National Healthcare Information Sharing and Analysis Center (NH-ISAC)
Scott Erven – Protiviti
Rick Hampton – Partners HealthCare System
Kevin Hemsley – Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) / DHS
Michael McNeil, MBA – Global Product Security and Services, Philips Healthcare
Kevin McDonald, BSN, ME-PD, CISSP – Mayo Clinic
Jeffrey Vinson – Information Security Department, Harris Health System

Session I Objectives:

1. Discuss the current cyber threat landscape within the healthcare and public health Sector (HPH)
2. Describe the current processes for sharing cyber threats
3. Identify lessons learned from the threats themselves as well as the subsequent threat response
4. Identify the impact of the threats and incidents to the HPH Sector

Questions for Consideration:

1. How are organizations currently receiving threat information? Do they belong to ISAOs? What threat feeds do they use?

2. How are organizations currently processing threat information?
3. Do organizations think they are receiving useful/actionable information?
4. What types of threats are healthcare organizations responding to?
5. How do you prioritize and assess the impact of the threats?
6. How do you raise awareness of the threat across healthcare organizations of varying size and resources?

Session II Plenary Panel (10:00am-11:30am) **– FDA's Current Thinking: Implementation of the NIST "Framework for Improving Critical Infrastructure Cybersecurity" for Strengthening Security Throughout the Total Product Life Cycle**

Moderator: Linda Ricci – Office of Device Evaluation (ODE) / CDRH / FDA

Session Discussants:

Denise Anderson, MBA – NH-ISAC
Seth Carmody, PhD – Office of In Vitro Diagnostics and Radiological Health (OIR) / FDA
Josh Corman – I am The Cavalry & Sonatype
Kevin Fu, PhD – Virta Labs & Archimedes Center for Medical Device Security, University of Michigan
Elisabeth George, MS – Philips Healthcare
Kevin Hemsley – ICS-CERT / DHS
Patrick Kehoe, MBA – Arxan
Ron Mehring, MBA, CISSP – Texas Health Resources
Colin Morgan, CISSP, GPEN – Information Security & Risk Management, Johnson & Johnson
John Murray, MS – Office of Compliance (OC) / CDRH /FDA
Henri "Rik" Primo, MS – Digital Health Services, Siemens Healthcare & Medical Imaging and Technology Alliance (MITA)
Zach Rothstein, JD – Technology & Regulatory Affairs, AdvaMed
Suzanne Schwartz, MD, MBA – Office of the Center Director (OCD) / CDRH / FDA
Ryan Winn – Information Systems, Munson Healthcare
Axel Wirth, CPHIMS, CISSP, HCISPP – Public Sector/Healthcare, Symantec Corp

Session II Objectives:

1. Inform key concepts of FDA's current thinking with respect to premarket and post market management of medical device cybersecurity:
    - 'Essential clinical performance' and potential impact on patient safety
    - Integration of threat modeling

- Information-sharing and timely remediation

2. Discuss stakeholders' interpretation and identify implementation challenges
3. Obtain input from healthcare and public health sector stakeholders on information sharing needs

Questions for Consideration:

1. How is the "Framework" incorporated into FDA's guidance for cybersecurity for premarket submissions?
    - How are firms addressing cybersecurity management in their premarket submissions?
2. How is the "Framework" being incorporated into FDA's postmarket management of medical device cybersecurity?
3. What should medical device vulnerability and threat information sharing look like? What information is to be shared and by whom?
4. What factors contribute to a manufacturer's decision whether or not to participate in an ISAO?
5. What are the characteristics (participation, expertise, policies, and practices) of an ISAO that would make it qualified to participate in the sharing and analysis of medical device cybersecurity vulnerabilities? What are the benefits and disadvantages of FDA "recognizing" specific ISAOs as possessing specialized expertise relevant to sharing and analysis of medical device vulnerabilities and what should such recognition entail?

BREAK (11:30am-11:40am)

ISAO Breakout Session (11:40am-12:40pm)

ISAO Breakout Session Objective

- Obtain additional feedback from stakeholders concerning outstanding questions regarding medical device information sharing.

Questions for Consideration:

1. If FDA is incentivizing industry to engage in information sharing with an ISAO, should that ISAO be "certified' by the FDA as meeting certain standards?
2. What structures ought to be considered as feasible for medical device vulnerability information sharing? Is a single medical device ISAO envisioned, or numerous ones perhaps funneling into a central center? In other words, how will this be architected?
3. Can we identify ISAO 'best practices' from other sectors that can be used in HPH?
4. Which best practices of threat information sharing are applicable to vulnerability information sharing?

5. What actionable information is necessary? What burden of proof is needed for escalation by ISAO? How is information vetted?
6. What should an ISAO be doing? Should the ISAO have an information validation component?
7. Should ISAOs have responsibility to push out information to ask their members about the pervasiveness of a vulnerability?
8. Initially an ISAO is clearing house of information. A more mature ISAO could have analysis capabilities. Where do we want to start and where do we want to end up?
9. What should the relationships between ISAOs potentially be? (e.g. National Council of ISAOs)

LUNCH (12:40pm-1:40pm)

Session III Plenary Panel (1:40pm-2:55pm) **– Key Ingredients for Effective Postmarket Management of Medical Device Vulnerabilities - Vulnerability Handling Processes and Coordinated Vulnerability Disclosure**

Moderator: Steve Christey Coley – Principal INFOSEC Engineer, Cybersecurity Division, The MITRE Corporation

Session Discussants:

Scot Copeland BSITSec, Sec+, MCP – Scripps Health

Allan Friedman, PhD – National Telecommunications and Information Administration (NTIA) / Department of Commerce

Kevin Hemsley – ICS-CERT / DHS

Art Manion – CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University

Michael McNeil, MBA – Global Product Security and Services, Philips Healthcare

Hannes Molsen, M.Sc. – Draeger & I Am The Cavalry

Katie Moussouris – HackerOne

Billy Rios, MBA, MSIS, CISSP – WhiteScope LLC

Suzanne Schwartz, MD, MBA – OCD / CDRH / FDA

Beau Woods – I Am The Cavalry

Session III Objectives:

1. Describe characteristics of coordinated vulnerability disclosure
2. Provide examples of tools and maturity models that may aid stakeholders in implementing coordinated disclosure and vulnerability management
3. Understand the roles and responsibilities of different stakeholders in vulnerability disclosure and management

Questions for Consideration:

1. How can stakeholder participation be incentivized? Which stakeholders should be providing incentives?
2. What do individual stakeholders need to understand and be aware of regarding coordinated disclosure?
3. What current tools and models presently exist that may aid stakeholders in implementing disclosure and vulnerability management? (e.g. ISO vulnerability disclosure model and the vulnerability coordination maturity model)
4. How might coordinated disclosure be operationalized? How do we ensure that accurate, actionable information is provided?
5. How can the security researcher community work in collaboration with HPH stakeholders to identify, assess, and mitigate vulnerabilities?
6. Should disclosure be made to the wider public or to more restricted groups?
7. How much detail needs to be disclosed?

BREAK (2:55pm-3:05pm)

Coordinated Vulnerability Disclosure Breakout Session (3:05pm-3:55pm)

Coordinated Vulnerability Disclosure Breakout Session Objective:

- Obtain additional feedback from stakeholders concerning outstanding questions regarding coordinated disclosure of medical device vulnerabilities.

Questions for Consideration:

1. Who should be vetting and validating medical device vulnerabilities?
2. Who do manufacturers want/need to coordinate vulnerabilities with (trade org, ISAO, ICS-CERT, researcher, etc.)?
3. What might be a good model for manufacturers to coordinate with these different entities?
4. Code of conduct: What do manufacturers expect of researchers? What do researchers expect of manufacturers?
5. Is disclosure of a vulnerability considered a complaint?
6. Do manufacturers have a distinct mechanism for collecting vulnerability information?
7. What can researchers do to have the greatest benefit to manufacturers while doing their research? (i.e. legacy vs. products in development)

Return from Breakout (3:55pm-4:05pm)

Session IV Plenary Panel (4:05pm-5:20pm) **– Overcoming Challenges Manufacturers Face with Increased Cybersecurity Collaboration**

Moderator: Zach Rothstein, JD – Associate Vice President, Technology & Regulatory Affairs, AdvaMed

Session Discussants:

Steve Abrahamson, BSME, MBA – GE Healthcare
Bill Aerts, CISSP, CISM – Global Privacy and Security Office, Medtronic
Carl Anderson, JD – Government Affairs, Health Information Trust Alliance (HITRUST)
Scot Copeland BSITSec, Sec+, MCP – Scripps Health
Allan Friedman, PhD – NTIA / Department of Commerce
Harley Geiger, JD, MA, CIPP/US – Rapid7
Ralph Hall, JD – Leavitt Partners & University of Minnesota
Kevin Hemsley – ICS-CERT / DHS
Marie Moe, PhD – Department of Software Engineering, Safety and Security, SINTEF ICT
Hannes Molsen, M.Sc. – Draeger & I Am The Cavalry
Katie Moussouris – HackerOne
Dale Nordenberg, MD – Medical Device Innovation, Safety, and Security Consortium (MDISS) & Novasano Health and Science
Bakul Patel, MS – OCD / CDRH / FDA
Billy Rios, MBA, MSIS, CISSP – WhiteScope LLC
Beau Woods – I Am The Cavalry

Session IV Objectives:

1. Provide examples of manufacturers interactions with different stakeholders as they work to address cybersecurity vulnerabilities
2. Identify lessons learned in taking a multi-stakeholder approach to addressing vulnerabilities

Questions for Consideration:

1. What lessons have been learned from these interactions thus far?
2. How does trust get established, especially if proprietary information is involved?
3. How might conflicts or differences of opinion be resolved (e.g. vulnerability severity, etc.)?
4. Knowing what you do now, how might you address interactions differently?

ISAO Breakout Report Out, Adjourn (5:20pm-5:35pm)

Principal Facilitators

Suzanne Schwartz, MD, MBA

Associate Director for Science and Strategic Partnerships, Acting Director Emergency Preparedness/Operations and Medical Countermeasures Program (EMCM), Center for Devices and Radiological Health (CDRH) Food and Drug Administration (FDA)

Day 2

Welcome, Coordinated Vulnerability Disclosure Breakout Report Out (Principal Facilitators),

Recap Day 1 (9:00am-9:35am)

Keynote Speaker (9:35am-9:55am)

Marty Edwards – Director Industrial Control Systems Cyber Emergency Response Team, National Cybersecurity and Communications Integration Center (NCCIC), Office of Cybersecurity and Communications (CS&C), Department of Homeland Security

Session V Plenary Panel (9:55am-10:55am) **– Identifying and Crafting Action Plans to Address Gaps and Challenges in Strengthening the Cybersecurity Stance of the Medical Device Ecosystem**

Moderator: Margie Zuk, MS – Senior Principal Cybersecurity Engineer, The MITRE Corporation

Session Discussants:

Scott Erven – Protiviti

Ben Flatgard, MA – National Security Council, White House

Jim Jacobson – Siemens Healthcare

Marie Moe, PhD – Department of Software Engineering, Safety and Security, SINTEF ICT

Iliana Peters, J.D., LL.M – Office of Civil Rights (OCR)

Linda Ricci – ODE / CDRH / FDA

Lucia Savage, JD – Office of the National Coordinator for Health Information Technology (ONC)

Roberto Suarez, HCISPP – Becton Dickinson

Jeffrey Vinson – Information Security Department, Harris Health System

Ryan Winn – Information Systems, Munson Healthcare

Session V Objectives:

1. Gain diverse perspectives on cybersecurity gaps and challenges that persist in medical devices across the total product lifecycle
2. Discuss ways the stakeholder community can begin addressing these gaps and challenges and what resources would be needed to do so

Questions for Consideration:

1. Remediation of vulnerabilities, what is acceptable and what is not?
2. Patches and updates for fixing security vulnerabilities – who receives? Should there be a cost to the customer? Who is the customer? How do customers who use third party servicing contracts

get the necessary fixes? What happens when components are no longer supported by manufacturers?

3. Should there be a Bill of Materials to account for all the components?
4. How might we address supply chain issues?
5. What about vulnerabilities that allow for breaches in PHI and PII? Are device manufacturers responsible?
6. How might we balance priorities of medical device vulnerabilities versus other cybersecurity/privacy issues faced by healthcare organizations?
7. Device manufacturers as 'business associates' to covered entities. What does that entail?
8. How can healthcare organizations cost-effectively assess the cybersecurity risk of devices during procurement?
9. How can products be designed to be part of a contested, inter-connected environment?
10. Outside of a regulatory context, what are the incentives that can be used to foster more secure medical devices?

BREAK (10:55am-11:05am)

Gaps & Action Plan Breakout Session (11:05am-12:15pm)

Gaps & Action Plan Breakout Session Objective:

- Ideate and discuss proposed solutions to specified cybersecurity gaps and challenges in the HPH ecosystem.

Questions for Consideration:

1. What are some approaches that may be utilized in the management of vulnerabilities across the total medical device product lifecycle (especially legacy devices)?
2. How might we best leverage cybersecurity researchers in the HPH ecosystem?
3. How might we more effectively share cybersecurity best practices and basic cyber hygiene concepts with stakeholders?
4. How might stakeholders collaborate to enhance cybersecurity testing capabilities?
5. How can we more accurately identify, understand, and portray the threat(s) so that manufacturers, HDOs, and researchers can make more informed risk management decisions, especially with respect to patient safety?

LUNCH (12:15pm-1:15pm)

Session VI Plenary Panel (1:15pm-2:15pm) – **Gaining Situational Awareness of the Current Activities in the HPH Sector to Enhance Medical Device Cybersecurity**

Moderator: Stephen Curren, MS – Office of Emergency Management (OEM) / Assistant Secretary for Preparedness and Response (ASPR) / HHS

Session Discussants:

Denise Anderson, MBA – NH-ISAC

Josh Corman – I am The Cavalry & Sonatype

Bryan Cline, PhD – HITRUST

Kevin Fu, PhD – Virta Labs & Archimedes Center for Medical Device Security, University of Michigan

Julian Goldman, MD – Partners HealthCare & Medical Device Interoperability Program

Ralph Hall, JD – Leavitt Partners & University of Minnesota

Lee Kim, BS, JD – Healthcare Information and Management Systems Society (HIMSS)

Deborah Kobza, CGEIT, JIEM – The Global Institute for Cybersecurity + Research (GICSR)

Marie Moe, PhD – Department of Software Engineering, Safety and Security, SINTEF ICT

Gavin O’Brien, MS – National Cybersecurity Center of Excellence (NCCoE), National Institute of Standards and Technology (NIST)

Dale Nordenberg, MD – MDISS & Novasano Health and Science

Session VI Objectives:

1. Provide examples of collaborative medical device and healthcare cybersecurity partnerships
2. Share lessons learned from collaborative approaches to medical device cybersecurity

Questions for Consideration:

1. What collaborations have various stakeholders been engaged in?
2. What gap(s) do these collaborations address? What challenges had or currently have to be overcome?

Session VII Plenary Panel (2:15pm-3:15pm) – **Risk Assessment Tools for the Medical Device Operational Environment**

Moderator: Marty Edwards, Director Industrial Control Systems, Cyber Emergency Response Team, National Cybersecurity and Communications Integration Center (NCCIC), Office of Cybersecurity and Communications (CS&C), Department of Homeland Security

Session Discussants:

Harold Booth – Computer Scientist, Computer Security Division (CSD) / Information Technology Laboratory (ITL), NIST

Penny Chase, MS, MA – Information Technology and Cybersecurity Integrator, The MITRE Corporation

Seth Carmody, PhD – OIR / FDA

Scott Erven – Protiviti

Rick Hampton – Partners HealthCare System

Dan Lyon – Principal Consultant, Cigital

Michael Murray – Director of Product Development Security, GE Healthcare

Henri “Rik” Primo, MS – Digital Health Services, Siemens Healthcare & MITA

Billy Rios, MBA, MSIS, CISSP – WhiteScope LLC

Roberto Suarez, HCISPP – Becton Dickinson

Axel Wirth, CPHIMS, CISSP, HCISPP – Public Sector/Healthcare, Symantec Corp

Session VII Objectives:

1. Raise awareness of the different risk assessment tools that may be leveraged
2. Identify key characteristics/components from risk assessment tools that may be used to describe the clinical environment
3. Identify challenge areas for risk assessment tools

Questions for Consideration:

1. What characteristics and/or components from CVSS might be leveraged in assessing vulnerability risk in the clinical environment?
2. What challenges exist in leveraging characteristics/components from CVSS and how might these be addressed?
3. What characteristics and/or components from other risk assessment tools might be leveraged in assessing vulnerability risk in the clinical environment?
4. What challenges exist in leveraging assessment tool characteristics/components and how might these be addressed?
5. How might we go about determining the clinical impact of a vulnerability? What questions need to be asked and which stakeholders are involved in this process?

BREAK (3:15pm-3:25pm)

Session VIII Plenary Panel (3:25pm-4:25pm) – **Adapting and/or Implementing Medical Device Cybersecurity Standards**

Moderator: Ken Hoyme, MS – Distinguished Scientist, Adventium Labs & Association for the Advancement of Medical Instrumentation (AAMI)

Session Discussants:

Brian Fitzgerald, B.Sc – Office of Science and Engineering Laboratories (OSEL) / CDRH / FDA

Anura Fernando, MS – Underwriters Laboratories

Kevin Fu, PhD – Virta Labs & Archimedes Center for Medical Device Security, University of Michigan

Michelle Jump, MS – Stryker Connected Care, Stryker Corporation

David Klonoff, M.D., FACP, FRCP (Edin), Fellow AIMBE – Diabetes Research Institute, Mills-Peninsula Health Services

Kevin McDonald, BSN, ME-PD, CISSP – Mayo Clinic

Michael McNeil, MBA – Global Product Security and Services, Philips Healthcare

Katie Moussouris – HackerOne

Gavin O'Brien, MS – NCCoE / NIST

Chana O'Leary, BSN, MA – TÜV Rheinland-OpenSky Corporation

Session VIII Objectives:

1. Discuss current cybersecurity standards and those in development
2. Discuss cybersecurity certification schemes for medical devices and/or hospital networks

Questions for Consideration:

1. What standards exist or are in development for cybersecurity risk management in medical devices? (e.g., AAMI TIR 57)
2. In addition to overarching cybersecurity standards, is there a need for device specific standards? If so, what might a device specific standard look like? (e.g., DTSec effort)
3. What is the role, if any, of cybersecurity certification schemes? What certification paradigms are currently being attempted and what lessons have been learned regarding the use of these paradigms for medical devices? (e.g. UL, TUV/Open Sky)
4. What challenges are encountered in the adoption of cybersecurity standards?

Day 2 Breakout Out Reports (Principal Facilitators), Workshop Recap, Closing Remarks (4:25pm-5:30pm)

Suzanne Schwartz, MD, MBA

Associate Director for Science and Strategic Partnerships, Acting Director Emergency Preparedness/Operations and Medical Countermeasures Program (EMCM), Center for Devices and Radiological Health (CDRH) Food and Drug Administration (FDA)

Speaker Biographies

Steven Abrahamson, MBA
Director of Product Security Engineering
GE Healthcare

Steven.Abrahamson@med.ge.com

Steve Abrahamson is Director of Product Security Programs at GE Healthcare, based in his hometown of Waukesha, Wisconsin. Steve established the Product Security program at GE Healthcare and has focused on implementing design engineering practices for security risk assessment and security controls integration within product designs. Steve promotes a security process that addresses risks to both patient safety and patient privacy, aligned with medical device regulatory requirements. Steve is also involved in collaborative efforts with other key healthcare stakeholders to find solutions for security challenges within the healthcare ecosystem. Steve is a frequent speaker at industry conferences and forums, including the FDA Workshop on Collaborative Approaches for Healthcare Cyber Security, US Information Security and Privacy Advisory Board, National Academy of Sciences Innovation Forum, HHS/NIST HIPAA Security Conference, HIMSS, mHealth, Advamed, AAMI, and the SANS Healthcare Cyber Security Summit.

Steve’s experience includes roles in Quality Assurance, Compliance, Continual Improvement, and Technical Management, and he is a certified Six Sigma Black Belt and Master Black Belt. Prior to joining GE Healthcare, Steve was a Quality Leader at GE Aviation, and prior to joining GE, Steve worked at Texas Instruments in their Defense Systems and Electronics group, supporting multiple precision-guided weapons programs including the HARM missile. Steve has a Bachelor’s Degree in Mechanical Engineering from Marquette University and a MBA from the University of Dallas. Steve also represents GE as a member of GE’s corporate marathon team, and he has completed over 120 marathons.

Bill Aerts, CISSP, CISM
Director, Product Security
Global Privacy and Security Office, Medtronic, plc

Bill Aerts is the Director of Product Security within Medtronic's Global Privacy and Security Office. In this role, Bill is accountable for the company-wide Global Product Security Program. The Program brings together the product R&D functions, security subject matter experts, and Business Unit and Corporate Leadership throughout the Company to continually improve security and privacy in the devices, systems, and services that Medtronic sells. To reach its goals, the global program drives the integration of security into product development, orchestrates Coordinate Response, monitors and influences the industry regarding medical device security, and provides security expertise to the business.

Bill has created and championed information and product security programs in the insurance, transportation, retail and healthcare industries throughout his 30+ years of experience working in Security roles. Bill received his bachelor's degree from the University of Wisconsin, and holds CISSP and CISM certifications.

Carl Anderson, J.D.
Vice President
Government Affairs
HITRUST

canderson@vsadc.com

Mr. Anderson has spent more than a dozen years in the Federal government and Capitol Hill. He specializes in the areas of cyber security, communications and information technology, healthcare policy, and energy policy.

Most recently, Mr. Anderson served as a counsel on the House Energy and Commerce Subcommittee on Oversight and Investigations. He was responsible for advising the Chairman and members of the Committee on issues occurring within the Committee's jurisdiction. Mr. Anderson tackled several high profile investigations and examined the growing world of cyber-threats and cyber-security.

Prior to joining the House and Energy and Commerce Committee, Mr. Anderson served at the U.S. Department of Justice in the Office of Justice Programs. There he managed a multitude of internal investigations, litigation and responded to congressional requests and investigations.

Prior to the Office of Justice Programs, Mr. Anderson served in the Civil Rights division at the Department of Justice. There he was responsible for prosecuting and negotiating settlements of housing discrimination cases. In this role, Mr. Anderson was appointed as a Special Assistant U.S. Attorney in the District of Columbia. As an Assistant U.S. Attorney, Mr. Anderson prosecuted dozens of active criminal cases in the District.

Mr. Anderson started his legal career at the U.S. Department of Justice in the Office of Legal Policy where he advised on a variety of policy matters, including the U.S.A. PATRIOT Act and the appointment of Article III judges.

Mr. Anderson is a frequent speaker on health information technology and cybersecurity, privacy and breach notification regulations.

Mr. Anderson graduated from Virginia Tech with a B.A. in Political Science and Columbus School of Law at the Catholic University of America with a Juris Doctor. He has been admitted to practice law in the District of Columbia.

Denise Anderson, MBA
Executive Director
National Health Information and Analysis Center
NH-ISAC

Denise Anderson has over 25 years of management level experience in the private sector and is Executive Director of the National Health Information Sharing and Analysis Center (NH-ISAC), a non-profit organization that is dedicated to protecting the health sector from physical and cyber attacks and incidents through dissemination of trusted and timely information.

Denise currently serves as Chair of the National Council of ISACs and participates in a number of industry groups such the Cross-Sector Cyber Security Working Group (CSCSWG). She was instrumental in implementing a CI/KR industry initiative to establish a private sector liaison seat at the National Infrastructure Coordinating Center (NICC) to enhance information sharing between the private sector, CI/KR community and the federal government and serves as one of the liaisons. She is a health sector representative to the National Cybersecurity and Communications Integration Center (NCCIC) — a Department of Homeland Security-led coordinated watch and warning center and sits on the Cyber Unified Coordination Group, (UCG) - a public/private advisory group that comes together to provide guidance during a significant cyber event.

Denise is certified as an EMT (B), Firefighter I/II and Instructor I/II in the state of Virginia, and is an Adjunct Instructor at the Fire and Rescue Academy in Fairfax County, Virginia. She is also certified under the National Incident Management System (NIMS). In addition, she has served on the Board and as Officer and President of an international credit association, and has spoken at events all over the globe.

Denise holds a BA in English, magna cum laude, from Loyola Marymount University and an MBA in International Business from American University. She is a graduate of the Executive Leaders Program at the Naval Postgraduate School Center for Homeland Defense and Security.

Harold Booth
Computer Scientist
Computer Security Division (CSD) / Information Technology Laboratory (ITL)
National Institute of Standards and Technology (NIST)

Harold Booth is a Computer Scientist at the National Institute of Standards and Technology (NIST). Harold is the project lead for the National Vulnerability Database (NVD) and is involved in the development of the Security Automation Program specifications.

Seth Carmody, PhD
Device Reviewer
Office of In Vitro Diagnostics and Radiological Health
Food and Drug Administration

Dr. Carmody joined the FDA's Center for Devices and Radiological Health in 2011 as a Staff Fellow in the Office of In Vitro Diagnostics and Radiological Health. Currently, Seth is a device reviewer in the Division of Chemistry and Toxicology Devices where his duties are focused mainly on premarket clearance/approval of diabetes-centric devices and software-related recalls. As a subject matter expert with CDRH's Cybersecurity Working Group, Seth is involved in Center policy development.

Penny Chase, MS, MA
Information Technology and Cybersecurity Integrator
The MITRE Corporation
pc@mitre.org

Penny Chase is the Information Technology and Cyber Security Integrator in the Information Technology Technical Center at The MITRE Corporation. In this role Penny promotes collaboration across MITRE's Information Technology and Cyber Security Technical Centers. Previously she was the Department Head for Human Language Technology within the Information Technology Technical Center. She has led MITRE and government-sponsored projects in developing structured representations for malware and threat information, security visualization, software assurance, malware analysis, reverse engineering, software architecture and design pattern recovery, network penetration testing, legacy database encapsulation, machine learning, and discourse-based natural language interfaces. Penny's research has been presented at dozens of conferences.

Penny is the Principal Investigator of a MITRE Sponsored Research Project on medical device security and safety, and supports MITRE's FDA/CDRH project on medical device cybersecurity. She is also the Principal Investigator of the Sharing Healthcare Fraud Data MSR. In addition, Penny leads the DHS Malware Attribute Enumeration and Characterization (MAEC) project for DHS. Previously she chaired the DHS/DOD/NIST Software Assurance Forum Working Group on Malware; served as the Deputy Director of the ARDA Northeast Regional Research Center, managing workshops that addressed Intelligence Community challenge problems; and was a member of the NASA Advisory Council's subcommittee on Avionics, Software, and Cybersecurity.

Penny received her Bachelor of Arts in Mathematics and History (with Harpur College Honors) from the State University of New York at Binghamton in 1975. She received her Master of Arts in the History of Science from Harvard University in 1976 and her Master of Science in Computer Science from Harvard University in 1986.

Steve Christey Coley
Principal INFOSEC Engineer
Cyber Security Division
The MITRE Corporation
coley@mitre.org

Steve Christey Coley is a Principal Information Security Engineer in the Cyber Security Division at The MITRE Corporation, supporting the FDA CDRH on Medical Device Cyber Security. He likes changing his last name every two decades or so. With cybersecurity experience dating back to 1993, Steve was the co-creator and Editor of the Common Vulnerabilities and Exposures (CVE) list and chair of the CVE Editorial Board from 1999 to 2015. He is the technical lead for the Common Weakness Enumeration (CWE), Common Weakness Scoring System (CWSS), and the community-driven CWE/SANS Top 25 Software Most Dangerous Software Errors. He was a co-author of the influential "Responsible Vulnerability Disclosure Process" IETF draft with Chris Wysopal in 2002. He was an active contributor to other efforts including the Common Vulnerability Scoring System (CVSS) version 2, the Common Vulnerability Reporting Framework (CVRF), NIST's Static Analysis Tool Exposition (SATE), certain non-public projects involving the assessment of static code analysis tools, and the SANS Secure Programming exams. His current interests include ensuring that emerging technologies do not repeat the chaotic path to effective vulnerability management that occurred with enterprise software in the 1990s; secure software development and testing; consumer-friendly software security metrics; the theoretical underpinnings of vulnerabilities; developing analogies between epidemiology and information security (e.g. within vulnerability statistics); improving the exchange of vulnerability information across global regions, language boundaries, emerging industries, and newly-connected technical domains; and making the cybersecurity profession more inclusive, diverse, and accessible to everybody who seeks a place in it. He holds a B.S. in Computer Science from Hobart College.

Bryan S. Cline, Ph.D.
Vice President
Standards and Analytics
Health Information Trust Alliance
Bryan.Cline@HITRUSTAlliance.net

Bryan Cline, Ph.D. is the Vice President of Standards and Analytics for the Health Information Trust Alliance (HITRUST) and provides thought leadership and guidance for the healthcare industry's model implementation of the NIST Cybersecurity Framework (CsF). Responsibilities include a broad range of HITRUST risk management framework support such as requirements integration, control specification, and the development of standards, methods, processes and tools that healthcare organizations can use to facilitate the integration and assessment of the CSF in their information protection and cybersecurity programs. As a former senior advisor and VP of CSF Development and Implementation, he worked closely with the Texas Health Services Authority (THSA) to develop SECURETexas—the first state program of its kind certifying compliance with federal and state requirements for the privacy and security of health information—and is considered the 'father' of the HealthCare Information Security and Privacy Practitioner credential for spearheading its development with (ISC)^2. Dr. Cline has also served as the Chief Information Security Officer for Catholic Health East and The Children's Hospital of Philadelphia in addition to his 20+ years in the Department of Defense as an information systems and information security professional, including the CISO role at the Headquarters, Allied Air Forces Southern Europe. He's spoken at multiple conferences and symposia on information security and privacy risk management in the healthcare industry and published articles and papers on risk management and security engineering in several journals and proceedings. Dr. Cline also co-chairs the Risk Management Sub-working Group of the Joint HPH Cybersecurity Working Group, which recently drafted NIST CsF implementation guidance for the HPH sector, and is currently working with THSA and the Texas Medical Association on additional guidance for small health organizations. His professional certifications include the CISSP-ISSEP, CISM, CISA, HCISPP, CCSFP, NSA IAM/IEM, MCIATT and DoD's CAP in project management.

Scot Copeland, BSITSec, MCP, Sec+
Medical I.T. Network Risk Manager
Scripps Health, San Diego, CA

Copeland.scot@scrippshealth.org

Scot Copeland currently serves in the role of Medical I.T. Network Risk Manager at Scripps Health in San Diego, California. With 20 years at Scripps Health, Scot is an industry leader in Medical Device Security/Risk Management and brings unique front-line experience from a Provider perspective. He has presented security and risk management topics on a national and local level. In 2015, he presented at the FDA, AAMI, American College of Clinical Engineers, HIMSS, California Medical Instrumentation Association, MedAssets and Biocom. He has also written and presented an exploration of socio-technological topics pertaining to medical device interoperability and the concept of a medical device network operating system.

Scot has extensive experience in identifying security and information risk issues in the clinical environment and has developed policies to evolve the Scripps Medical Equipment Management Plan toward information security maturity. As a member of the Scripps I.T. Policies Workgroup he helped update and develop the I.T. Risk Management policies and standards to include medical device modalities. Scot served as project lead in the implementation of the IEC80001:2010 frame work for Medical I.T. Network Risk Management as Scripps Health became a test and development site for early adoption.

Scot originally served as a radio repairman in the U.S. Marine Corps and first obtained certification as a Certified Biomedical Engineering Technician in 1992. He has recently returned to college and obtained a Bachelor’s Degree in Information Technology Security from Western Governors University specifically for application to medical device and clinical technology issues. He retains the responsibility of Clinical Systems Specialist Lead responsible for administering the Medical Equipment Management Plan at Scripps/Mercy Hospital, Chula Vista, CA and still troubleshoots and repairs medical device systems from time to time.

Josh Corman
Founder I Am The Cavalry
Chief Technology Officer
Sonatype

Joshua Corman is a Founder of I Am The Cavalry (dot org) and the CTO for Sonatype. Corman has served key research and strategy roles at Akamai Technologies, The 451 Group, and IBM Internet Security Systems. He co-founded @RuggedSoftware and @IamTheCavalry to encourage new security approaches in response to the world's increasing dependence on digital infrastructure. Josh's unique approach to security in the context of human factors, adversary motivations and social impact has helped position him as one of the most trusted names in security. He is an adjunct faculty for Carnegie Mellon's Heinz College and Advisor to DHS S&T. Josh received his bachelor's degree in philosophy, graduating summa cum laude, from the University of New Hampshire.

Stephen Curren, MS
Director, Division of Resilience and Infrastructure Coordination
Office of Emergency Management
Office of the Assistant Secretary for Preparedness and Response
U.S. Department of Health and Human Services (HHS)

Steve Curren leads the Continuity of Operations (COOP) and Critical Infrastructure Protection (CIP) programs within U.S. Department of Health and Human Services (HHS), through which he works to build organizational resilience for all threats and hazards faced by HHS and the broader Healthcare and Public Health Sector. Since his arrival at HHS in 2008, Steve has focused on a wide range of critical infrastructure matters, including physical security, cybersecurity, supply chain continuity, business continuity, pandemic preparedness, extreme weather preparedness, and other areas of risk management. He served as lead for the Department in the development and implementation of policies such as Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience, Executive Order 13636 on Improving Critical Infrastructure Cybersecurity, and the Protection Framework developed under Presidential Policy Directive 8 (PPD-8). In all of these efforts, he has focused on partnership, information sharing, and collaboration among public and private sector entities to advance shared security and resilience goals.

Prior to joining ASPR, Steve worked five years at the Association of State and Territorial Health Officials (ASTHO), where he served as Senior Director for Public Health Preparedness. At ASTHO he directed a program to develop and disseminate model policies and practices to advance public health preparedness for state and territorial public health agencies.

Steve began his career as an industry consultant on public health and regulatory policy issues, with a focus on U.S. and European regulatory affairs. He holds a Bachelor of Science degree in Biology from Wake Forest University and Master of Science in Foreign Service (MSFS) degree from Georgetown University with Honors in International Business Diplomacy. He has completed executive crisis leadership training through Harvard University’s National Preparedness Leadership Initiative and the Foreign Service Institute’s National Security Executive Leadership Seminar.

Marty Edwards
Director Industrial Control Systems Cyber Emergency Response Team
National Cybersecurity and Communications Integration Center (NCCIC)
Office of Cybersecurity and Communications (CS&C)
Department of Homeland Security

Marty Edwards is the Director of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), an operational division of the department's National Cybersecurity and Communications Integration Center (NCCIC) and the DHS Office of Cybersecurity and Communications (CS&C)

ICS-CERT works to reduce industrial control system risks within and across all critical infrastructure and key resource sectors by coordinating efforts among federal, state, local and tribal governments, as well as industrial control systems owners, operators and vendors. In collaboration with the other NCCIC components the ICS-CERT responds to and analyzes control systems related incidents, conducts vulnerability and malware analysis, and shares and coordinates vulnerability information and threat analysis through products and alerts.

Mr. Edwards has over 20 years of experience and brings a strong industrial control system industry focus to DHS. Before coming to the ICS-CERT, Mr. Edwards was a program manager focused on control systems security work at Idaho National Laboratory. Prior to his work at the laboratory, Mr. Edwards held a wide variety of roles in the instrumentation and automation fields, including field service, instrument engineering, control systems engineering and project management.

Mr. Edwards has also held various positions in nonprofit organizations, including Chairman of the Board for one of the automation communities' largest user group conferences. Mr. Edwards holds a diploma of technology in Process Control and Industrial Automation (Magna cum Laude) from the British Columbia Institute of Technology.

The ICS-CERT is the recipient of the 2013 SC Magazine Security Team of the Year award.

Scott Erven
Associate Director
Protiviti

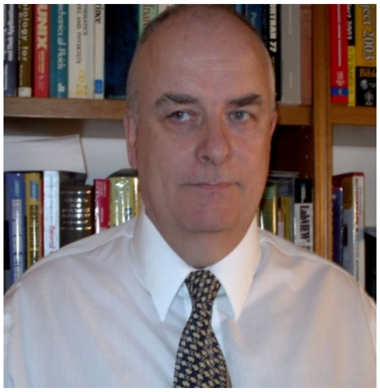
Scott Erven is a security researcher and consultant. He has more than 15 years of information security and information technology experience with subject matter expertise in medical device and healthcare security. Scott has spent over 5 years managing information security programs for large healthcare systems. His research on medical device security has been featured in Wired and numerous media outlets worldwide. Mr. Erven has presented his research and expertise in the field internationally. Scott also has served as a subject matter expert and exam writer for numerous industry certifications. His current focus is on research that affects human life and public safety issues inside today's healthcare landscape.

Anura S. Fernando, MS
Principal Engineer for Medical Software & Systems
Underwriters Laboratories

Anura S. Fernando is UL's Principal Engineer for Medical Software & Systems Interoperability.

He holds degrees in Electrical Engineering, Biology/Chemistry, and Software Engineering. Anura has over 18 years of experience at UL with safety critical software and control systems certification and has also conducted research across multiple application domains – industrial automation, alternative energy, medical, hazardous locations, appliances, optical radiation, nanotechnology, battery technologies, etc. He has been involved in the development of Safety Science and generated publications in Predictive Modeling and Risk Analysis, Cybersecurity, Systems of Systems, Software, Health IT, Apps, and Medical Device safety. Anura has been engaged in projects with numerous Fortune 500 companies, DoD, DoE, DHS, FDA, FCC, ONC, NASA, and several U.S. National Laboratories. He has contributed to the development of several standards involving software and Functional Safety as a member in IEC, ISO, ASME committees and served as an IECEE Expert Task Force member. Anura currently has global responsibility for medical device software certification at UL and serves as UL's technical lead for the development of the AAMI/UL 2800 family of eHealth standards for interoperable medical device interface safety and the UL 2900-2-1 Cybersecurity standard for healthcare. He has served as a member of the Federal Advisory Committee FDA Safety and Innovation Act WG, FDA Medical Device Interoperability Coordinating Council, Medical Device Interoperability Safety Working Group, NIH QMDI Program Advisory Committee, the Association for the Advancement of Medical Instrumentation, HIMSS, and the International Council on Systems Engineering, along with IEC and ISO where he is involved with a number of interoperability-related committees.

Brian Fitzgerald, B.Sc
Senior Technical Manager HPC and Cybersecurity
Office of Science and Engineering Laboratories
Food and Drug Administration
Brian.fitzgerald@FDA.hhs.gov



Brian Fitzgerald was educated in England and received his engineering degree from University College Cardiff in Wales. He became a US citizen in 2003.

He left the private sector in 1992 after a multidisciplinary engineering career, and joined Underwriters Laboratories (UL) in Raleigh, NC helping to start their software safety initiative. He has contributed to the development of several national and international standards for programmable systems UL 1998, IEC 60601-1-4, AAMI SW68 and most recently IEC 62034, IEC 80001 and IEC ACSEC Guide for Privacy and Security. He was nominated as a US National Expert by AAMI to WG22 of IEC SC62a dealing with programmable systems, to ISO TC210 WG1 dealing with quality systems and to JWG7 of IEC and ISO for Medical IT networks.

He is a member of the AAMI software committee, the AAMI IT committee and the AAMI Cybersecurity committee. Prior to joining FDA he was an accredited software expert and lead auditor for two European notified bodies. He continues to conduct public seminars in software safety, risk management, medical device cybersecurity, software related regulatory affairs and medical quality systems. He is a member of the US National Council of the International Electrotechnical Commission.

He joined FDA's CDRH in October 2003 in the Office of Science and Engineering Laboratories to specialize in systems, software evaluation and safety research activities. He is currently Senior Technical Manager for Cybersecurity and High Performance Computing.

Current projects include researching the use of formal methods as they relate to generalized 'assurance cases' including safety cases and compliance cases, and the development of forensic techniques for detecting and investigating software failure. He leads the technical and research aspects of the FDA cybersecurity team. He is active in the internal governance structures of FDA computational science and manages both the FDA's new high performance computing center and semantic text mining activities. He continues to contribute to FDA Guidance development, product review activities and works with several other Federal Regulatory Agencies in the field of cybersecurity.

Ben Flatgard, MA
Director for Cybersecurity Policy
National Security Council (NSC)
White House

Ben Flatgard serves as Director for Cybersecurity Policy on the National Security Council. In this role, he is responsible for developing policy that will enhance the cybersecurity of critical infrastructure and increase the effectiveness of cybersecurity information sharing. Prior to joining the NSC staff, Ben served as Senior Advisor for Financial Institutions at the U.S. Treasury Department. He previously worked for the Secretary of Commerce and in the White House.

Allan Friedman, PhD
Director of Cybersecurity
National Telecommunications and Information Administration
U.S. Department of Commerce
afriedman@ntia.doc.gov

Allan Friedman is the Director of Cybersecurity Initiatives at National Telecommunications and Information Administration in the US Department of Commerce. He coordinates NTIA's multistakeholder process on security research vulnerability disclosure. Prior to joining the Federal government, Friedman was a noted cybersecurity and technology policy researcher. Wearing the hats of both a technologist and a policy scholar, his work spans computer science, public policy and the social sciences, and has addressed a wide range of policy issues, from privacy to telecommunications. Friedman has over a decade of experience in cybersecurity research, with a particular focus on economic, market, and trade issues. He has a degree in Computer Science from Swarthmore College, a PhD in Public Policy from Harvard University, and is the coauthor of Cybersecurity and Cyberwar: What Everyone Needs to Know (Oxford University Press, 2014).

Kevin Fu, PhD
Associate Professor,
Chief Scientist Virta Labs and Director Archimedes Center for Medical Device Security
University of Michigan

fugistics@umich.edu

Dr. Kevin Fu is credited for establishing the field of medical device security beginning with the 2008 IEEE paper on defibrillator security. Kevin is Chief Scientist of Virta Labs, Inc. and Associate Professor in EECS at the University of Michigan where he directs the Archimedes Center for Medical Device Security and the Security and Privacy Research Group (SPQR) at secure-medicine.org.

Kevin has testified in the House and Senate on matters of information security and has written commissioned work on trustworthy medical device software for the Institute of Medicine of the National Academies. He has briefed White House staff on methods to improve medical device security. Kevin was named MIT Technology Review TR35 Innovator of the Year. Kevin served as program chair of USENIX Security, a member of the NIST Information Security and Privacy Advisory Board, and co-chair of the AAMI Working Group on Medical Device Security. He served as a visiting scientist at the Food & Drug Administration, the Beth Israel Deaconess Medical Center of Harvard Medical School, Microsoft Research, and MIT CSAIL. Kevin received his B.S., M.Eng., and Ph.D. from MIT. He earned a certificate of artisanal bread making from the French Culinary Institute.

Harley Lorenz Geiger, JD, MA, CIPP/US
Director of Public Policy
Rapid7

@HarleyGeiger

Harley Geiger is Director of Public Policy at Rapid7.

Prior to working at Rapid7, Harley was Advocacy Director and Senior Counsel at the Center for Democracy & Technology (CDT) from 2014-2016. He worked on issues related to civil liberties and government surveillance, computer crime, and cybersecurity. From 2012-2014, Harley served as Senior Legislative Counsel for U.S. Representative Zoe Lofgren of California. There he was the lead staffer for technology and intellectual property issues. Before working on the Hill, Harley was Staff Attorney and Senior Policy Counsel at CDT from 2008-2012. Harley is CIPP/US certified.

Elisabeth M. George, MS
Vice President of Global Regulation & Standards
Philips Healthcare

Elisabeth has a BS in Biomedical Engineering from Boston University and MS in Engineering Management from Northeastern University. She has worked in Medical Device Regulatory for more than 25 years. Her carrier began as a biomedical engineer in Boston Children's Hospital and then as a design engineer in Control Systems Engineering for Power Plants. She then held a number of positions in design, operations, quality and test engineering for military electronics before moving into Medical Devices where she has held positions in R&D, Operations and Quality/Regulatory.

Today, Elisabeth works for Philips managing and supporting the strategic planning & technical aspects in the areas of quality, regulatory, security & sustainability for more than 30 design & manufacturing facilities around the world. She is responsible for technical teams ensuring compliance & improvement in regulations, standards and guidance documents development, awareness and deployment in supporting product submissions, post market surveillance, product reliability, quality systems (ISO13485, 21CFR), environmental management system (ISO14001 & OHSAS 18001), software development and security requirements & business systems. Philips product portfolio includes: X-Ray, MRI, CT and Nuc Med Systems, Generators, Tubes and Components, Home & Patient Solutions and supporting Information Systems along with their associated supplies and services as well as a plethora of consumer products (e.g.; Sonicare Toothbrushes, Humidifiers, Coffee makers). She has participated in multiple FDA Advisory Panels as the Manufacturer's Representative.

She actively participates in industry groups and standards organizations domestically and internationally including: ANSI,AAMI, NEMA, MITA, MDMA, Eucomed, COCIR and AdvaMed. She actively represents Philips and Industry as a whole in technical activities including US Access Board Advisory Committee in 2012-2013 on Imaging Systems as well as on the 2013 FDASIA 618 HIT Policy Working Group. She is an active member in standards groups(AAMI, ANSI & NEMA) including as a member of the USNC, USNC-CAPCC and USNC-IECEE as well as a number of international committees. She has presented at industry forums and to government and regulatory agencies around the world including in China, Brazil, India, Europe, Japan and Korea.

Julian M. Goldman, MD
Medical Director of Biomedical Engineering for Partners HealthCare
Anesthesiologist, Massachusetts General Hospital
Director, Medical Device Interoperability Program
jmgoldman@mgh.harvard.edu

Dr. Goldman is the Medical Director of Biomedical Engineering for Partners HealthCare, an anesthesiologist at the Massachusetts General Hospital, and Director/PI of the Program on Medical Device Interoperability (MD PnP) - a multi-institutional research program founded in 2004 to advance medical device interoperability to improve patient safety and HIT innovation.

Dr. Goldman performed his clinical and research training at the University of Colorado, and is Board Certified in Anesthesiology and Clinical Informatics. He served as a Visiting Scholar in the FDA Medical Device Fellowship Program as well as an executive of a medical device company. At MGH, Dr. Goldman served as a principal anesthesiologist in the “OR of the Future” - a multi-specialty clinical testbed that evaluated diverse technologies and clinical practices prior to broad adoption.

Dr. Goldman chairs the international standardization committee for the safety and performance of anesthesia and respiratory equipment (ISO TC 121), and serves in leadership positions of AAMI, UL, and IEC standardization committees. He Co-Chaired the HHS HIT Policy Committee FDASIA Regulations Subcommittee and the FCC mHealth Task Force, and co-chairs the healthcare group of the Industrial Internet Consortium.

Dr. Goldman’s awards include the AAMI Technology in Health Care Clinical Application Award, the International Council on Systems Engineering Pioneer Award, the American College of Clinical Engineering award for Professional Achievement in Technology, and several American Society of Anesthesiologists awards for advanced technology applications to improve patient safety.

Ralph Hall, JD
Partner, Leavitt Partners
Professor of Practice, University of Minnesota

Ralph Hall is a partner at Leavitt Partners and works in the Washington, D.C., office. In this role, Ralph provides policy and consulting services to clients in the areas of FDA statutes and regulations, regulatory compliance and health care policy and legislation. He is particularly focused on the application of those regulatory systems to the medical device industry. He is actively involved in heading several alliances working to improve key FDA regulatory and statutory process.

Ralph furthermore has served as a Professor of Practice at the University of Minnesota Law School for more than a decade. In this role, he concentrates his teaching, research and writing in the area of FDA law, health care compliance and negotiations. He has published numerous academic articles and serves as the faculty editor-in-chief of the Minnesota Journal of Law, Science and Technology.

In addition, Ralph is Of Counsel with Faegre Baker Daniels. Through the law firm he provides clients with legal services primarily related to FDA matters, corporate compliance, the design and implementation of cross-disciplinary corporate legal strategies, and general corporate counseling.

Ralph has an extensive background with drug and medical device regulation and corporate compliance matters. He has spent many years in industry. Ralph has served in a succession of high-level positions with Guidant Corporation and Eli Lilly and Company including serving as the General Counsel of a billion dollar operating unit and as Chief Compliance Officer.

He received his B.A. from Indiana University and his juris doctorate from the University of Michigan where he was a Weymouth Kirkland Scholar.

Rick Hampton
Wireless Communications Manager
Partners HealthCare System, Boston, MA
rhampton@partners.org

Rick Hampton is the Wireless Communications Manager for Partners HealthCare System, Inc., Boston, MA. Rick is responsible for the overall coordination of activities relating to the safe, effective and secure use of all wireless communications technologies at Partners HealthCare and its affiliates. This includes selecting and designing state-of-the-art systems, educating staff on wireless technologies, resolving electromagnetic compatibility, interference and health issues, addressing cybersecurity issues and developing policies and procedures. Rick also works with patient safety, industry and regulatory bodies to develop responses to these issues and is heavily involved in safety, security and risk management standards for medical devices.

Rick has a B.S. in Biomedical Engineering from Wright State University, Dayton, Ohio. His healthcare experience includes fifteen years as a paramedic and nearly 30 years as a clinical engineer in large healthcare companies. His wireless background includes over 40 years working with military, commercial, amateur, consumer and medical systems.

Rick is involved in numerous projects to raise the awareness of healthcare professionals and manufacturers regarding wireless systems in healthcare facilities. Among them are the AAMI EMC Committee, Mobile Healthcare Alliance efforts to develop a white paper on wireless use in hospitals and an IEEE RF Wireless Working Group developing guidance on the usage of radio-frequency wireless communication technologies for IEEE 1073 point-of-care medical devices that exchange vital signs and other medical device information using shared information technology infrastructures. Lately, he has been busy with the IEC 80001 standards group to develop a risk-management model when connecting medical devices to general-purpose IT LANs. He has also consulted with hospitals on medical telemetry and communications technologies.

Kevin Hemsley, CISSP
Project Manager
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
National Cybersecurity and Communications Integration Center (NCCIC)
Industrial Control Systems Cyber Emergency Team (ICS-CERT)
Department of Homeland Security

Kevin Hemsley is a project manager at the Idaho National Laboratory supporting the US Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) which is an operational division of the National Cybersecurity and Communications Integration Center (NCCIC) (Pronounced N-Kick).

ICS-CERT works to reduce control systems risks within and across all critical infrastructure and key resource sectors including the Healthcare and Public Health Sector by coordinating efforts among federal, state, local and tribal governments, as well as control systems owners, operators and vendors. In collaboration with the other NCCIC components the ICS-CERT responds to and analyzes control systems related incidents, conducts vulnerability and malware analysis, and shares and coordinates vulnerability information and threat analysis through alerts and advisories.

Mr. Hemsley manages various DHS-related projects at the INL including oversight of the Vulnerability Handling team that works with independent security researchers and control system device vendors from around the world to identify and mitigate vulnerabilities affecting US critical infrastructure. ICS-CERT coordinates medical device vulnerabilities for the US Department of Homeland Security. Mr. Hemsley has more than 20 years of experience in cyber security ranging from network security to control system and medical device security.

Ken Hoyme, MS
Distinguished Scientist
Adventium Labs
ken.hoyme@adventiumlabs.com

Mr. Hoyme has over 30 years' experience in the design and development of safety-critical, real-time, fault-tolerant and secure systems in a variety of regulated domains, including medical systems, commercial and military avionics, industrial automation and space systems. He is a recognized expert in the field of systems engineering.

Mr. Hoyme is the co-chair of the AAMI Device Security working group, which is developing guidance for the application of medical safety risk standard ISO 14971 to security risk management and serves on AAMI's Systems Engineering Advisory Board.

At Adventium Labs, Mr. Hoyme's research focus is on safety and security-critical architectures and risk management methods for cyberphysical systems in a variety of domains, including medical devices. He is leading research efforts that focus on meeting both safety and security requirements both at the device level and when integrating several devices into an integrated clinical environment.

Prior to joining Adventium Labs, Mr. Hoyme was a Senior Fellow at Boston Scientific where he was the systems lead for the development of the LATITUDE Remote Patient Management system. He was also the technical focal for developing standards for interconnecting implantable cardiac device data to electronic medical records systems.

Prior to joining Boston Scientific, Ken spent 18 years at Honeywell's Corporate Research lab, where he was a Senior Fellow in their real-time computer systems group. He was awarded the H.W. Sweatt Award, Honeywell's highest technical recognition for his work on the Boeing 777.

Ken has been granted 34 US patents. He is a member of IEEE and INCOSE. He received the Bachelors and Masters Degrees in Electrical Engineering from the University of Minnesota.

Jim Jacobson
Chief Product and Solution Security Officer
Siemens Healthcare

Jim Jacobson is the Chief Product and Solution Security Officer for Siemens Healthcare. Since 2012, he has been responsible for the global security program for the medical devices and associated IT systems, solutions and services that Siemens Healthcare develops, sells, maintains and supports. He is also responsible for the internal processes that protect the privacy of the patient data the products generate. Jim also sits on the Siemens Product and Solution Security Board responsible for governance and guidance for the security of the company's products, solutions and services in all sectors including industrial, power, energy, renewables and mobility, in addition to healthcare. He leads the board's work team responsible for the curriculum and training program in this area for Siemens employees worldwide. Prior to these roles, Jim has led medical device-related software development teams in ultrasound, laboratory diagnostics and informatics since 1990 at Siemens and other companies. Jim completed the bachelors program in physics at Oberlin College.

Michelle L. Jump, MS, RAC
Principal Regulatory Affairs Specialist
Stryker Connected Care
Stryker Corporation
michelle.jump@stryker.com

Michelle Jump is a Principal Regulatory Affairs Specialist at Stryker Corporation, with over 15 years of experience in the regulated health industry. She serves as an internal technical expert, advising development teams and management on technical standards and regulatory strategy for software, security, mobile apps, emerging technology, and connected devices. Ms. Jump has a passion for bringing technology-based solutions to healthcare, actively participating in a variety of international and domestic standards development work, as well as serving as a panel member, session leader, and presenter at a variety of events to further solutions to the challenges of technology in healthcare.

Current leadership roles in the area of standards development include Project Lead for ISO Joint Working Group 7 Foundational Document (IEC 62304 and IEC 80001) as well as the Project Lead for the new AAMI Technical Information Report 75: Factors to Consider when Multi-Vendor Devices Interact via an Electronic Interface. Ms. Jump is the co-chair of the AdvaMed Software Working group and the co-chair of the AAMI Health Software Quality working group. She is also a member of the AAMI Standards Board and has participated as the primary U.S. industry representative for the International Medical Device Regulators Forum (IMDRF) on the Software as a Medical Device working group. At Stryker, Ms. Jump chairs 3 cross-divisional working groups in (1) interoperability, (2) security, and (3) software.

Ms. Jump holds a Master of Science in Regulatory Science from the University of Southern California and a Master of Science in Biotechnology from California State University. She is also RAC certified.

Patrick Kehoe, BS / Computer Science and MBA
CMO
Arxan

pkehoe@arxan.com

Mr. Kehoe and the team at Arxan are in the business of understanding application security vulnerabilities and deploying approaches to protect applications -- building on over 10 years of research and intellectual capital on this topic.

Mr. Kehoe brings over twenty years of experience working with software, hardware, and service providers in the High Tech and security industry.

His work in the medical device and healthcare market is focused on:

•Minimizing threats to patient health and safety that can result from application tampering and malicious attacks

•Ensuring the privacy and confidentiality of medical health records and data via state-of-the-art whitebox cryptography

•Preventing the disassembly or decompilation of applications or application logic that can expose the IP within applications

•Ensuring that the mobile apps that doctors/payers/patients are using are protected from attacks and that the environment in which mobile apps are running has not be compromised

Patrick holds a degree in Computer Science from Vanderbilt University and a MBA from the Darden Graduate School of Business at the University of Virginia.

Lee Kim, JD, FHIMSS
Director of Privacy and Security
Healthcare Information and Management Systems Society (HIMSS)

lkim@himss.org

Lee Kim is the Director of Privacy and Security at the Healthcare Information and Management Systems Society (HIMSS) and a Fellow of HIMSS. HIMSS is a global, cause-based, not-for-profit organization focused on better health through information technology (IT). HIMSS leads efforts to optimize health engagements and care outcomes using information technology.

Kim is a member of the National Association of State Chief Information Officers (NASCIO) Health Care Working Group and the SANS Securing the Human Healthcare advisory board. Kim is a licensed attorney in the District of Columbia and Pennsylvania. Kim is admitted to practice before the Federal Circuit and the United States Patent and Trademark Office as a registered patent attorney.

She holds an AV Preeminent® peer review rating in health care and intellectual property from Martindale-Hubbell. Kim's publications have included articles in E-Commerce Law & Policy, E-Finance & Payments Law & Policy, and a chapter in the American Bar Association book, Health Care IT: The Essential Lawyer's Guide to Health Care Information Technology and the Law. Previously, Kim worked as a healthcare and intellectual property attorney in private practice and as a technologist in the healthcare and information technology industries.

David C. Klonoff, M.D. FACP, FRCP (EDIN), Fellow AIMBE
Medical Director
Diabetes Research Institute
Mills-Peninsula Health Services
dklonoff@diabetestechnology.org

David C. Klonoff, M.D. is a practicing endocrinologist specializing in diabetes technology. He is Medical Director of the Diabetes Research Institute at Mills-Peninsula Health Services (Sutter Health) in San Mateo, California and a Clinical Professor of Medicine at UCSF. Dr. Klonoff received an FDA Director's Special Citation Award in 2010 for contributions related to diabetes technology. He has been cited as being in the top 1% of endocrinologists nationally by Castle Connolly Medical Ltd. In 2012 Dr. Klonoff was elected as a Fellow of the American Institute of Medical and Biological Engineering (AIMBE) and cited as one of the top 2% of the world's bioengineers for his engineering work in diabetes technology. He received the 2012 Gold Medal Oration and Distinguished Scientist Award from the Dr. Mohan's Diabetes Specialities Centre and Madras Diabetes Research Foundation of Chennai, India. In 2015 Dr. Klonoff was invited to participate in the White House Health and Cybersecurity Roundtable for developing policies related to the healthcare sector and the Precision Medicine Initiative. He is the Founding Editor-in-Chief of Journal of Diabetes Science and Technology. He has authored over 230 publications, including articles on cybersecurity for diabetes devices, insulin pump safety, medjacking, mHealth, and precision medicine. Dr. Klonoff founded MEDSec – the Medical Device Cybersecurity and Privacy Meeting.

Dr. Klonoff is a graduate of UC Berkeley, where he was elected to Phi Beta Kappa in his junior year, and UCSF Medical School, where he was elected to Alpha Omega Alpha in his junior year. His postgraduate training included two years at UCLA Hospital and three years at UCSF Hospitals. Dr. Klonoff currently chairs the consensus multiagency DTSec Program (Diabetes Technology Society Cybersecurity Standard for Connected Diabetes Devices), whose Standard and Protection Profile are currently out for public review. This program was featured in Wired Magazine in 2015.

Deborah Kobza, CGEIT, JIEM
President/CEO
The Global Institute for Cybersecurity + Research (GICSR)
NASA/Kennedy Space Center
Deborah.Kobza@gicsr.org

Deborah Kobza, as President/CEO of the Global Institute for Cybersecurity + Research, leads a public/private critical infrastructure partnership to advance critical infrastructure resilience. In partnership with NASA/Kennedy Space Center and in collaboration with the U.S. Department of Homeland Security, NIST, government agencies, academia and private industry, GICSR serves as the trusted international collaborative facilitating open dialogue, critical insight and thought exchange linking critical infrastructure stakeholders to define and deliver scalable, flexible and adaptable cybersecurity resilience solutions.

Utilizing GICSR's G3 (Global Cooperation, Collaboration & Coordination), GICSR leverages a foundational three-tiered approach to advance cyber resilience: NIST "Framework for Improving Critical Infrastructure Cybersecurity", NIST "National Cybersecurity Workforce Framework, and The Global Cyber Range (CRi – Cyber Research Innovation; C3i - Intelligence, Information Sharing & Response – National Cyber First Responders; CSD - Cybersecurity Secure Design (Modeling, Simulation, Testing); and CyPRO – Cyber Professional Education & Virtual Range.

25+ years of experience includes strategic alignment of business and technology domains, IT governance, computer systems validation, quality assurance, security, workforce education, and development of public/private partnerships supporting leading practice applied research and adoption, critical infrastructure protection, information sharing and coordinated response.

Deborah founded the National Health Information Sharing & Analysis Center (NH-ISAC), serving as Executive Director from 2010 to 2015. In collaboration with the FDA (NH-ISAC/FDA MOU) and the medical device community, Mrs. Kobza led NH-ISAC in supporting development of a Medical Device Cybersecurity Framework and to address reporting and remediation of medical device vulnerabilities.

Prior, Mrs. Kobza served as CEO of the IT Center of Excellence, and provided consulting services to the U.S. Department of Homeland Security, state governments and private industry.

Deborah serves on various cybersecurity working groups with the U.S. Department of Homeland Security, Department of Defense, and private industry, including serving as Chair of the Global Forum to Advance Cyber Resilience.

Dan Lyon
Principal Consultant
Cigital, Inc
dlyon@cigital.com

Dan Lyon is a Principal Consultant with Cigital, one of the world's largest consulting firms on application security, where he leads the embedded and medical device practices.

Prior to Cigital, Dan spent 18 years with Medtronic building medical device software for implants, programmers, and network services. He performed software, system and security engineering and led multiple projects from feasibility to market release. Achievements included a nomination for Technical Contributor of the Year.

Dan has actively participated in AAMI's Device Security working group and IEEE's Building Code for Medical Device Software Security.

Dan holds BA degrees in Mathematics and Computer Science from Luther College, as well as five active certifications through GIAC.

Art Manion
Senior Vulnerability Analyst
CERT Coordination Center
Software Engineering Institute, Carnegie Mellon University
amanion@cert.org

Art Manion is a senior member of the Vulnerability Analysis team in the CERT Coordination Center, part of the Software Engineering Institute at Carnegie Mellon University. He has studied vulnerabilities and coordinated responsible disclosure efforts since joining CERT in 2001. After gaining mild notoriety for saying "Don't use IE" in a conference presentation, Manion now focuses on policy, advocacy, and rational tinkering approaches to software security, including standards development in ISO/IEC JTC 1 SC 27 Security techniques. Prior to joining CERT Manion was the Director of Network Infrastructure at Juniata College.

Kevin McDonald, BSN, ME-PD, CISSP
Director of Clinical Information Security
Office of Information Security
Mayo Clinic
McDonald.Kevin@mayo.edu

Kevin McDonald is the Director of Clinical Information Security at Mayo Clinic. His current responsibilities include the security of medical devices, environmental systems and clinical support systems across the Mayo Clinic sites. Kevin and his team provide testing, mitigation and consultative services for devices and systems within Mayo Clinic and partner with external vendors to assist them in improving the security of their products. Their work has become nationally recognized with presentations at the Radiologic Society of North America Conference, Gartner Security and Risk Management Summits, AdvaMed MedTech, NH-ISAC Summit, Archimedes Workshop and many others. Kevin also participates in, and brings Mayo Clinic's experiences to, several vendor security customer advisory boards. Kevin has over 35 years of healthcare experience in both patient care and technology roles. His experience includes critical care and emergency nursing, nursing management, electronic medical record implementation, information technology and information security. He has an undergraduate degree in Nursing and graduate degrees in Education and Information Systems.

Michael McNeil, MBA
Global Product Security & Services Officer
Royal Philips Healthcare

Michael C. McNeil is the current Global Product Security & Services Officer for Royal Philips. In this capacity, McNeil is responsible for leading the global product security program for the company and insuring consistent repeatable processes are deployed throughout their products and services in the Healthcare market. Prior to this assignment, McNeil was the former Global Chief Privacy & Security Officer at Medtronic responsible for the development and design of their initial product security and incident response management programs; Chief IT Security Officer at Liberty Mutual Group; Global Chief Privacy Officer at Pitney Bowes, and Vice President, Chief Privacy Officer of Data Services for Reynolds & Reynolds.

McNeil is a noted security and privacy expert, he has conducted in-house training and presentations for industry, customers and clients and has presented at several security and privacy conferences worldwide. Michael is a current Governing Body Co-Chair for the annual Summit, Boston and Minneapolis CISO Executive Summits presented by Evanta. He is an active member of the Association for the Advancement of Medical Instrumentation (AMMI), Medical Device Safety & Security Consortium (MDISS), and the NH-ISAC. Michael has held the chair position for the Medical Device Privacy Consortium (MDPC) and currently holds the chair position for the MDPC Device Security Working Group which recently published the Whitepaper entitled "Security Risk Assessment Framework for Medical Devices".

He was recently named an inaugural, 2013 Top 10 Breakaway Leader of Chief Information Security Officer (CISO), and was also awarded in 2013 as the First Minneapolis CISO Visionary Award, in addition to these accomplishments, he was also awarded the 2011 Outstanding MBA of the Year by the National Black MBA Association.

Michael is married to Devita McNeil and they are the proud parents of two children (Danielle and Vincent) and grandfather of Jadyn.

Ron Mehring, MBA, CISSP
Vice President – Technology & Security
Texas Health Resources

RonaldMehring@texashealth.org

Ron Mehring serves as the Vice President of Technology & Security for Texas Health Resources, one of the largest faith-based, nonprofit health care delivery systems in the United States. The system's primary service area includes 16 counties in north-central Texas, home to more than 6.2 million people.

At Texas Health Resources, Ron leads Technology Operations, IT Risk Management & Assurance, IT BC DR program and Technology & Security Performance and Standards teams.

Ron began his career in technology for the United States Marine Corps. After 21 years of military service, Ron retired from the Marine Corps and joined the Department of Veteran Affairs where he led Compliance Assessment teams within the newly formed Oversight & Compliance group. He also served as the Department of Veterans Affairs' Deputy Director for Network & Security Operations.

Ron holds an MBA in Risk Management from NYIT and is a Certified Information Systems Security Professional (CISSP).

Marie Moe, PhD
Research Scientist
Department of Software Engineering, Safety, and Security
SINTEF ICT
marie.moe@sintef.no

Dr. Marie Moe is passionate about incident handling and information sharing, she cares about public safety and securing systems that may impact human lives, this is why she has joined the grassroots organization "I Am The Cavalry".

Marie is a Research Scientist at SINTEF ICT, and has an MSc in Mathematics and a PhD in Information Security. She has experience as a team leader at NorCERT, the Norwegian National CERT (Computer Emergency Response Team). Marie also holds a position as Associate Professor at NTNU, the Norwegian University of Science and Technology, where she supervises students and teaches a class on incident management and contingency planning.

Marie's life depends on the working of a medical device, a pacemaker that generates every single beat of her heart. As a security-professional Marie is worried about her heart's attack surface. How can she trust the machine inside her body, when it is running on proprietary code and there is no transparency? This is why she acquired medical devices that can communicate with her pacemaker, and started a project on investigating the security of her medical implant, together with a team of volunteer hackers.

This awareness-raising research project has gained much interest and she has become a sought-after speaker on the topic of medical implant privacy and security. She did a keynote talk on living with a vulnerable medical device at the hacker-conference Hack.lu, she was invited to give a guest lecture at the University of Cambridge and she also presented her research project at the biggest European hacker-congress CCC in December 2015.

Hannes Molsen, M.Sc.
Product Security Manager
Dräger
i am the cavalry
hannes.molsen@draeger.com

Hannes Molsen is the global Product Security Manager of Dräger, a 125 year old family company known, e.g., for medical devices and safety systems. He is responsible for creating and maintaining an environment which enables Dräger to ship devices and applications that are secure to sustain in an interconnected world, throughout the entire system's lifecycle, to protect life, data and system functionality.

At Draeger as well as during his activities as self-employed Security Professional he also tests devices and applications, and gives security trainings for developers, product managers and software architects.

Before taking this position, he was working as a passionate secure coder, with over 10 years of experience in web application development, software for embedded systems and interconnected devices.

He is also actively involved with the grass roots organization i am the cavalry, supporting the efforts to connect manufacturers and the security research community to become safer, sooner, together.

Hannes holds a Master of Science degree in Computer Science from the Hamburg University of Technology.

Colin Morgan, CISSP, GPEN
Head of Global Product Security
Information Security & Risk Management
Johnson & Johnson
cmorga48@its.jnj.com

Colin Morgan, Johnson & Johnson Information Security & Risk Management, is leading the company's Global Product Security initiative to integrate cybersecurity into the Johnson & Johnson product development lifecycle and post market surveillance processes. This effort is focused on developing fundamental cybersecurity policies, standards and processes; establishing integral partnerships with both internal and external organizations; driving education and awareness plans; and monitoring and assessing industry and regulatory trends. Colin has worked in the cybersecurity field for a number of organizations including the Central Intelligence Agency and the National Oceanic & Atmospheric Administration. He is a featured speaker on cybersecurity and is passionate about the integration of the competency across all industries. Colin has his Bachelor's degree in Computer Engineering from The College of New Jersey, a Master's degree in Telecommunications from George Mason University, and is CISSP and GPEN certified.

Katie Moussouris
Chief Policy Officer
HackerOne
Katie@hackerone.com

Katie Moussouris is the Chief Policy Officer for HackerOne, a platform provider for coordinated vulnerability response & structured bounty programs. She is a noted authority on vuln disclosure & advises lawmakers, customers, & researchers to legitimize & promote security research & help make the internet safer for everyone. Katie's earlier Microsoft work encompassed industry-leading initiatives such as Microsoft's bounty programs & Microsoft Vulnerability Research. She is also a subject matter expert for the US National Body of the International Standards Organization (ISO) in vuln disclosure (29147), vuln handling processes (30111), and secure development (27034). Katie is a visiting scholar with MIT Sloan School, doing research on the vulnerability economy and exploit market. She is a New America Foundation Fellow. Katie is an ex-hacker, ex-Linux developer, and persistent disruptor. Follow her and HackerOne on Twitter http://twitter.com/k8em0 and http://twitter.com/hacker0x01

John F. Murray Jr., MS
Expert Regulatory Review Scientist
Office of Compliance
Center for Devices and Radiological Health
United States Food and Drug Administration

Mr. Murray serves as an Expert Regulatory Review Scientist with United States Food and Drug Administration. His day to day work is focused on the interpretation and application of FDA Regulations for FDA Regulated Computer and Software Products.

In addition to his 20 years at FDA, John's professional experience includes the United States Navy Nuclear Submarine Service, Telex Computer Products, General Dynamics Corporation, and Technology Management & Analysis.

Mr. Murray earned his Bachelor of Science in Electronics Engineering from George Mason University and his Master of Science in Computer Science from Rensselaer Polytechnic Institute.

Michael Murray
Director of Product Development Security
GE Healthcare

Michael Murray is the Director of Product Development Security at GE Healthcare, responsible for providing secure design and secure development expertise and services to support GE Healthcare's engineering teams across the product development lifecycle. A career information security professional, Michael has taken leadership roles in organizations ranging from small consulting firms to Fortune 100 companies. Before joining GE, Michael was co-founder and managing partner of MAD Security / The Hacker Academy. He holds a BA in Philosophy from the University of Toronto.

Dale Nordenberg, MD
Executive Director, MDISS
CEO, Novasano Health and Science

dalenordenberg@novasano.com

Dr. Nordenberg is CEO of Novasano Health and Science, a company that delivers information technology services and products to accelerate innovation in healthcare and life sciences. He has extensive experience in healthcare strategy and operations, health information technology, FDA regulated industries, research network development, public-private partnership development, and emergency preparedness.

Dr. Nordenberg is co-founder and Executive Director for the Medical Device Innovation, Safety, and Security Consortium (MDISS), a public-private partnership that works with device manufacturers, healthcare systems, government agencies, and other stakeholders to improve the security and safety of medical devices and biomedical device networks. He serves on the Brookings Institute Medical Device Post Market Surveillance System Planning Board and recently coordinated a National Academy of Sciences Innovation Policy Forum briefing on medical device innovation.

Prior to Novasano, Dr. Nordenberg was a managing director in the health care practice of PricewaterhouseCoopers. From 2002 through 2007, he was the Chief Information Officer and Associate Director, National Center for Infectious Diseases and was detailed to the Office of the National Coordinator for Health Information Technology. He was a member of the Science and Technology Review Subcommittee of the Science Advisory Board of the FDA, 2007 and 2009. Prior to CDC, Dr. Nordenberg was a founding executive of a company that launched VeriSign affiliates in Latin America and Asia; faculty in the Emory School of Medicine where he founded and directed the Office of Medical Informatics for the Emory University Children's Center and was the physician informatics lead at Eglest on Children’s Hospital.

Dr. Nordenberg is a pediatrician, medical epidemiologist and medical informaticist. He completed a BS in Microbiology from the University of Michigan, medical degree from Northwestern University, pediatrics residency at McGill University (Montreal Children’s Hospital), and fellowship in epidemiology in the Epidemic Intelligence Services Program at the Centers for Disease Control.

Gavin O’Brien, MS
Computer Scientist
National Institute of Standards and Technology (NIST)
National Cybersecurity Center of Excellence (NCCoE)

Gavin O’Brien is a computer scientist with the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST). He launched the center’s first health IT use case and, since early 2013, has been overseeing a use case for mobile device security.

Prior to joining the NCCoE in 2012, Mr. O’Brien spent 13 years at NIST’s IT Laboratory where he spent much of his time working on healthcare testing tools. While working with groups inside the Nationwide Health Information Network (NwHIN), he also participates as a monitor for the IHE USA North American Connectathon.

Before his career with NIST, Mr. O’Brien worked in the startup community during the dot-com era in the mid 90’s for a few B2B companies. Mr. O’Brien received a bachelor’s of science in mathematics from Bates College and subsequently earned a master’s degree in computer science from the University of Tennessee.

Chana L. O'Leary, BSN, MA
Senior Security Consultant
TÜV Rheinland-OpenSky Corporation
coleary@openskycorp.com

Chana (pronounced "Hah-nah") O'Leary is a member of the Eastern region division of TÜV Rheinland-OpenSky Corporation in their IT Risk Management (ITRM) practice. She has deep knowledge of securing n-tier architectures, application security, security requirements elicitation and threat modeling. Her current interests include exploring the topics of usable security, secure software `source software in medical devices and the design of usable and secure user interfaces. She is a former Lead Architect for KLM/Air France and a Technology Manager with BearingPoint, BV. She also teaches Big Data security at Austin Community College as Adjunct Faculty. One of the hats she most enjoys wearing is that of mentor/teacher to development teams and students around the world. She has a Bachelor's degree in Nursing, an MA from UNISA in Psychology and a graduate certificate in Usability Engineering from the University of Washington. She is a member of the Cloud Security Alliance, a member of the Working Group on Big Data for NIST and a member of ISECOM, the open source security group.

Stephen Ostroff, MD
Commissioner (Acting)
Food and Drug Administration

Dr. Stephen Ostroff, M.D., has been FDA's Acting Commissioner since April 2015.

Previously, he was FDA's Chief Scientist, where he was responsible for leading and coordinating FDA's cross-cutting scientific and public health efforts. The Office of the Chief Scientist works closely with FDA's product centers, providing strategic leadership and support for FDA's regulatory science and innovation initiatives.

Dr. Ostroff joined FDA in 2013 as Chief Medical Officer in the Center for Food Safety and Applied Nutrition and Senior Public Health Advisor to FDA's Office of Foods and Veterinary Medicine.

Prior to that, he served as Deputy Director of the National Center for Infectious Diseases at the Centers for Disease Control and Prevention (CDC). He retired from the Commissioned Corps of the U.S. Public Health Service at the rank of Rear Admiral (Assistant Surgeon General).

Dr. Ostroff was the Director of the Bureau of Epidemiology and Acting Physician General for the Commonwealth of Pennsylvania and has consulted for the World Bank on public health projects in South Asia and Latin America.

Dr. Ostroff graduated from the University of Pennsylvania School of Medicine in 1981 and completed residencies in internal medicine at the University of Colorado Health Sciences Center and preventive medicine at CDC.

He is a fellow of the Infectious Disease Society of America and the American College of Physicians, and prior to assuming the role of FDA's Acting Commissioner, he chaired the Public Health Committee of the American Society for Microbiology's Public and Scientific Affairs Board.

Bakul Patel, MSEE, MBA
Associate Director for Digital Health
Office of the Center Director
Center for Devices and Radiological Health (CDRH)
U.S. Food and Drug Administration (FDA)
bakul.patel@fda.hhs.gov

BAKUL PATEL is Associate Director for Digital Health (acting), at the Center for Devices and Radiological Health (CDRH), at the Food and Drug Administration (FDA). Mr. Patel leads regulatory policy and scientific efforts at the Center in areas related to emerging and converging areas of medical devices, wireless and information technology. This includes responsibilities for mobile health, health information technology, cyber security, medical device interoperability, and medical device software.

Mr. Patel is the FDA liaison between the Federal Communications Commission (FCC) and the Office of the National Coordinator (ONC). Since its inception in 2013, Bakul chairs the International Medical Device Regulators Forum (IMDRF) "software as a medical device" working group, a global harmonization effort.

Before joining FDA, Mr. Patel held key leadership positions working in the telecommunications industry, semiconductor capital equipment industry, wireless industry and information technology industry. His experience includes Lean Six Sigma, creating long and short-term strategy, influencing organizational change, modernizing government systems, and delivering high technology products and services in fast-paced, technology-intensive organizations.

Mr. Patel earned an MS in Electronic Systems Engineering from the University of Regina, Canada, and an MBA in International Business from The Johns Hopkins University.

Iliana L. Peters, J.D., LL.M
Senior Advisor for HIPAA Compliance and Enforcement
Office of Civil Rights

Iliana L. Peters is the Senior Advisor for HIPAA Compliance and Enforcement at the HHS Office for Civil Rights. In this role, Ms. Peters is the national lead for OCR enforcement of the HIPAA Rules, and works closely with OCR's ten regional offices to promote compliance with and enforcement of the HIPAA Rules. Additionally, she supports many other OCR policy and outreach initiatives, including rulemakings, compliance initiatives with other federal agencies, and training, including of the State Attorneys General. Prior to joining the team in D.C., Ms. Peters worked as an investigator in Region VI in Dallas, Texas. Ms. Peters received her Law Degree from Duke and her Masters of Law in Health Care Law from the University of Houston's Health Law and Policy Institute. Prior to joining OCR, she worked in private practice in Texas.

Henri "Rik" Primo, MS.
Director Strategic Relationships
Digital Health Services
Siemens Healthcare
rick.primo@siemens.com

Henri "Rik" Primo manages Strategic Relationships for Siemens Digital Health Services in USA. Primo's career with Siemens started in 1998 as Marketing Manager in the Health Services Division. His general expertise with digital imaging, PACS and healthcare information systems proved invaluable in this position. Prior to his career in the RIS/PACS/CVIS/RIS domains, Primo managed the Biomedical Engineering and Electronic Data Processing Departments at the 500-bed Holy Family Hospital in Ghent, Belgium. Primo served as faculty member at numerous RIS/PACS events. He has been a featured speaker at the Society of Imaging Informatics in Medicine (SIIM), TEPR (USA), MSRT, CARS, RSNA, PACS 2000, AHRA, ACR, NYMIIS, NCHICA and other professional Societies and Organizations on the topic of digital imaging, digital imaging workflow, big data, cybersecurity and PACS in general. He holds patents for film digitizing technologies. He provided education on Digital Radiology at the University of Charleroi in Belgium from 1985 to 1988. Primo assumed the function of Secretary and Director-at-Large on the board of the Society of Imaging Informatics (SIIM) for six years. He is currently the Chairman of the Medical Imaging Technology Alliance (MITA) Medical Imaging Informatics section, member of the MITA Board of Directors and Siemens-elected voting member of the Internet of Things council at the National Electrical Manufacturers Association (NEMA).

Henri is member of the Siemens' Strategic Standards Management Council and provides guidance to Siemens executive management on Imaging Informatics standards, policies and technologies.

A native of Ghent, Belgium, Primo holds a degree in electrical engineering from the city's Institute of Technology. He resides in Chicago, Illinois with his wife, Stephanie. Henri enjoys listening to music, exploring the graphic arts and touring the world on his short-wave amateur radio station.

Linda Ricci
Biomedical Engineer
Office of Device Evaluation
Food and Drug Administration

Linda Ricci began her career developing artificial intelligence solutions in the defense industry. In this role she designed and developed software implementations of neural network applications. Ms. Ricci then moved to the medical device industry as a software engineer. She helped to develop several diagnostic cardiology devices and has participated in all phases of product life cycle development. Ms. Ricci moved to the FDA in 2005 first as a scientific reviewer and then as the Chief for the Cardiac Diagnostic Devices Branch in the Division of Cardiovascular Devices. In this role, she was responsible for the review of devices including automated external defibrillators, electrocardiographs, multi-parameter monitors and non-invasive blood pressure monitors. Currently Ms. Ricci leads the development and implementation of digital health policy within the Office of Device Evaluation. She has degrees in Electrical Engineering and Medical Engineering.

Billy Rios
Founder
WhiteScope LLC
Contact@whitescope.io

Billy is the founder of Whitescope LLC, a startup focused on embedded device security. Billy is recognized as one of the world's most respected experts on emerging threats related to Industrial Control Systems (ICS), Critical Infrastructure (CI), and, medical devices. He discovered thousands of security vulnerabilities in hardware and software supporting ICS and critical infrastructure. He has been publicly credited by the Department of Homeland Security (DHS) numerous times for his support to the DHS ICS Cyber Emergency Response Team (ICS-CERT). He is credited with providing the technical research leading to the first FDA cyber security safety advisory. Billy has worked at Google where he led the front line response for externally reported security issues and incidents. Prior to Google, Billy was the Security Program Manager at Internet Explorer (Microsoft). During his time at Microsoft, Billy led the company's response for several high profile incidents, including the response for Operation Aurora.

Billy is a contributing author to Hacking: The Next Generation, The Virtual Battlefield, and Inside Cyber Warfare. He currently holds a Master of Science in Information Systems, an MBA, and a Masters of Military Operational Arts and Science.

Zachary Rothstein, JD
Associate Vice President
Technology & Regulatory Affairs
Advamed

zrothstein@advamed.org

Zach Rothstein is Associate Vice President for Technology & Regulatory Affairs at the Advanced Medical Technology Association (AdvaMed). In this position, Zach advocates for medical device regulatory policies that are transparent, predictable, consistent, timely, and science-based, with an emphasis on U.S. Food and Drug Administration ("FDA") and legislative activities. Zach's particular areas of focus include digital health, medical device software, cybersecurity, labeling, and postmarket surveillance.

Prior to joining AdvaMed, Zach was Deputy Senior Counsel for Public Policy at Samsung Electronics where he was responsible for the company's medical device and healthcare regulatory and policy issues. In this position, Zach counseled Samsung's global business units through all stages of product development on U.S. regulations affecting digital health, Health IT, and medical devices. Zach also planned and executed the company's FDA and healthcare regulatory and legislative policy objectives. While at Samsung, Zach served on the Board of Directors for the Personal Connected Health Alliance (formerly Continua) and the Consumer Electronics Association's Health and Fitness Technology Division.

Prior to joining Samsung, Zach was an Attorney in the FDA and Healthcare practice at the law firm of Morgan, Lewis & Bockius LLP. In this role, Zach served as outside counsel to various healthcare companies on FDA and HHS regulatory, compliance, and enforcement matters.

Zach earned his J.D. from The Catholic University of America, where he was a Notes and Comments Editor of the Law Review, President of the Moot Court Board, and won first place and best brief awards at the 2009 National Telecommunications Moot Court Competition. Zach received his B.A. in political science and criminal justice from Indiana University, Bloomington.

Zach is an active member of the Food and Drug Law Institute, teaches an introduction to FDA law class at the Johns Hopkins University, and was recognized by i3 magazine as a digital health and fitness innovator.

Lucia C. Savage, JD
Chief Privacy Officer
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
Lucia.savage@hhs.gov

Lucia Savage, Esq. was appointed Chief Privacy Officer at Office of the National Coordinator for Health Information Technology, Department of Health & Human Services in October 2014, Lucia Savage has been working on health privacy, transparency, and interoperable health information exchange since HIPAA was enacted. In 2015, Ms. Savage was the architect of the privacy and security provisions of ONC's "A Shared Nationwide Interoperability Roadmap (October 2015)" as well as its updated "Guide to Privacy & Security of Electronic Health Information (April 2015)". She has helped develop the final Privacy Principles for the Precision Medicine Initiative. And, she advises the National Coordinator for Health IT and others on the privacy and security in the next phase of health IT, using apps, mobile health, APIs, and other emerging technologies.

She previously served as General Counsel at Pacific Business Group on Health and California's former health insurance exchange, PacAdvantage. Most recently, as Senior Associate General Counsel at UnitedHealthcare she advised regarding large data transactions, health information exchange, and APCDs.

Lucia has a BA with Honors from Mills College in Oakland, CA, and received her Juris Doctor summa cum laude from New York University School of Law.

Suzanne B. Schwartz, MD, MBA
Associate Director for Science and Strategic Partnerships
Director (Acting) Emergency Preparedness/Operations and Medical Countermeasures (EMCM)
Center for Devices and Radiological Health
U.S. Food and Drug Administration

Suzanne.Schwartz@fda.hhs.gov

Suzanne B. Schwartz, MD, MBA is the Associate Director for Science and Strategic Partnerships in the Center for Devices and Radiological Health (CDRH) at the FDA. She also serves as the Director (Acting) of CDRH's Emergency Preparedness/Operations and Medical Countermeasures program. Suzanne represents CDRH/FDA across inter-Agency initiatives for the Public Health Emergency Medical Countermeasures Enterprise (PHEMCE) for chemical, biological, radiological and nuclear threats (CBRN), natural disasters and emerging infectious diseases.

In her role as CDRH's Emergency Operations Coordinator, Suzanne is responsible for preparedness and incident response to matters concerning cybersecurity of medical devices and their networked systems. Her programmatic efforts have evolved beyond response to include increasing awareness, educating, outreach, partnering and coalition-building within the Healthcare and Public Health Sector (HPH). Suzanne chairs the CDRH Cybersecurity Working Group which is tasked with formulating policy on medical device cybersecurity on behalf of the Agency. She also serves as co-chair of the Government Coordinating Council (GCC) for the HPH Critical Infrastructure Sector.

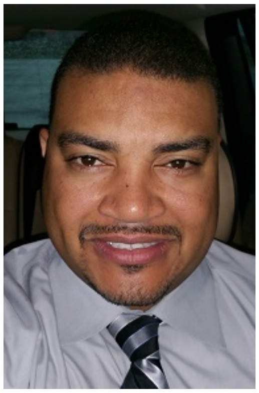
Suzanne earned an MD from Albert Einstein College of Medicine of Yeshiva University in New York in 1988, trained in General Surgery and Burn Trauma; an executive MBA from NYU Stern School of Business in 2012, and completed Cohort X of the National Preparedness Leadership Initiative – Harvard School of Public Health & Harvard Kennedy School of Government executive education in June 2013.

Roberto Antonio Suárez, HCISSP
Product Security Manager
BD

Roberto Suárez is a product security and privacy professional in the medical device and healthcare IT industry. At BD, Roberto is responsible for developing a Product Security Center of Excellence that drives process, capability and maturity to build products that are secure by design with transparency and control in mind. Giving product teams exposure to cyber security training and events, building their in-house expertise and promoting a company-wide community for product security is what Roberto is passionate about. Roberto started his career in the Software Engineering department of Siemens Corporate Research and then worked on remote service platforms for medical devices in Siemens Healthcare Diagnostics. Through his technical knowledge acquired during these experiences and his personal initiative, Roberto became a Product Security Expert and Program Manager for Siemens Healthcare where he educated product development teams on product security activities, institutionalized policies and procedures as well as supported secure product design and architecture. He is a Certified HealthCare Information Security and Privacy Professional (HCISPP) and has degrees in Computer Science from Montclair State University.

Jeffery M. Vinson, C|CISO, CISSP, NSA IAM/IEM
Vice President & Chief Information Security Officer (CISO)
Information Security Department
Harris Health System

Jeffrey.vinson@harrishealth.org



Jeffrey Vinson, Sr. is the Vice President and Chief Information Security Officer at Harris Health System. A former Technical Director at NSA, he has been involved with information security for over 20 years and has the rare distinction of having expert experience in the military, federal government, financial services and healthcare industries. He has held positions such as Vice President, Information Security; Technical Director, Vulnerability Assessments; CISO and other senior level security management roles. Jeffrey has led penetration testing exercises while working at NSA (National Security Agency) as a Technical Director and has created security operations teams for financial services and healthcare organizations. He provides expert security advice and guidance to small and large companies and speaks at security conferences throughout the country. Jeff is a member of C|CISO exam writing and events committee for EC-Council and was one of their first C|CISO summit speakers for their global CISO Executive Summit

Ryan Winn
Director
Information Systems
Munson Healthcare
rwinn2@mhc.net

Ryan Winn has 15+ years experience in healthcare IT. He is currently the Director of Information Services at Munson Healthcare in Traverse City, Michigan. At Munson, he has responsibility for all technical functions plus information security and privacy for the health system. Prior to joining Munson, he worked in leadership positions at MidMichigan and Banner Health. During his career, he has provided leadership to many large initiatives including EMR implementations in both acute and ambulatory settings, systems integration, facility acquisitions, information security and strategic planning. He earned his BS in Management of Information Systems from University of Colorado, Denver.

Axel Wirth, MSc, CPHIMS, CISSP, HCISPP
Distinguished Technical Architect
Public Sector/Healthcare
Symantec Corporation
axel_wirth@symantec.com

As Solutions Architect, Axel Wirth provides strategic vision and technical leadership within Symantec's Healthcare Vertical, serving in a consultative role to healthcare providers, industry partners, and health technology professionals.

Drawing from over 25 years of international experience in the industry, Mr. Wirth is supporting Symantec's healthcare customers to solve their critical security, privacy, compliance, and IT management challenges. He is an active participant in industry organizations and a frequent speaker at conferences, forums, and webcasts on subjects such as cybersecurity, medical device security, mobile health infrastructure, compliance automation, IT infrastructure optimization, and other healthcare-specific topics.

His extensive background in the healthcare IT and medical device industries includes engineering leadership as well as strategic business development and marketing roles with Siemens Medical, Analogic Corp., Mitra Inc., Agfa Healthcare, and currently Symantec Corp. His education includes a BS Electrical Engineering degree (EE) from Fachhochschule Düsseldorf and an MS Engineering Management degree (MSEM) from The Gordon Institute of Tufts University.

Beau Woods
I Am The Cavalry

Beau Woods is a core contributor to the grassroots initiative, I Am The Cavalry, ensuring connected technology that can impact life and safety is worthy of our trust. Beau has over a decade in Cyber Security, and has advised dozens of organizations on security practice, strategy and technology, including Global 100, small businesses, NGOs, government agencies, and others. Beau is a frequent presenter, media contributor, and author. He received Bachelor of Science in Psychology from the Georgia Institute of Technology.

Margie Zuk, MS
Senior Principal Cyber Security Engineer
The MITRE Corporation

mmz@mitre.org

Margie Zuk is a Senior Principal Cyber Security Engineer at the MITRE Corporation, with over 30 years of cyber security experience. She is currently the Cyber Engagement Lead for Healthcare in the Cyber Security Technical Center, where she leads MITRE's support to the FDA CDRH on Medical Device Cyber Security.

As the Industry Collaboration Department Head for many years, Margie led MITRE's work in cross sponsor initiatives and cyber partnerships providing expertise in Threat Based Defense, Cyber Threat Intelligence, Security Automation, Software Assurance, Privacy, and Social and Behavioral Science. Margie led the evolution of the cyber standards work at MITRE from the launch of CVE to the recent structured threat work with STIX and TAXII for DHS. She developed trusted partnerships with senior leaders across government and industry to establish governance models and to evolve the cyber security standards strategy. Prior to this, Margie led MITRE's support to the National Information Assurance Partnership (NIAP). She was an initial member of the Common Evaluation Methodology Editorial Board, and participated in the development of the US scheme for the Common Criteria.

Margie has a Bachelor of Arts in Mathematics from the College of Mt. St. Vincent and a Master of Science in Computer Science from Stevens Institute of Technology.

[Federal Register Volume 80, Number 76022 (Monday, December 7, 2015)]

[Notices]

[Pages 76022-76025]

From the Federal Register Online via the Government Printing Office [www.gpo.gov]

[FR Doc No: 2015-30772]

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration [Docket No. FDA-2014-N-1286]

Moving Forward: Collaborative Approaches to Medical Device Cybersecurity; Public Workshop; Request for Comments
AGENCY: Food and Drug Administration, HHS.
ACTION: Notice of public workshop; request for comments.

The Food and Drug Administration (FDA) is announcing the following public workshop entitled "Moving Forward: Collaborative Approaches to Medical Device Cybersecurity." FDA, in collaboration with the National Health Information Sharing Analysis Center (NH-ISAC), the Department of Health and Human Services, and the Department of Homeland Security, seek to bring together diverse stakeholders to discuss complex challenges in medical device cybersecurity that impact the medical device ecosystem. The purpose of this workshop is to highlight past collaborative efforts; increase awareness of existing maturity models (*i.e.* frameworks leveraged for benchmarking an organization's processes) which are used to evaluate cybersecurity status, standards, and tools in development; and to engage the multi-stakeholder community in focused discussions on unresolved gaps and challenges that have hampered progress in advancing medical device cybersecurity.

Dates and Times: The public workshop will be held January 20-21, 2016, from 9 a.m. to 5:30 p.m. Submit either electronic or written comments on the public workshop by February 22, 2016.

Location: The public workshop will be held at the FDA White Oak Campus, 10903 New Hampshire Ave., Building 31 Conference Center, the Great Room, (Rm. 1503), Silver Spring, MD 20993-0002. Entrance for the public meeting participants (non-FDA employees) is through Building 1 where routine security check procedures will be performed. For parking and security information, please refer to *http://www.fda.gov/AboutFDA/WorkingatFDA/BuildingsandFacilities/WhiteOakCampusInformation/ucm241740.htm*.

You may submit comments as follows:

Electronic Submissions

Submit electronic comments in the following way:

- Federal eRulemaking Portal: *http://www.regulations.gov*. Follow the instructions for submitting comments. Comments submitted electronically, including attachments, to *http://www.regulations.gov* will be posted to the docket unchanged. Because your comment will be made public, you are solely responsible for ensuring that your comment does not include any confidential information that you or a third party may not wish to be posted, such as medical information, your or anyone else's Social Security number, or confidential business information, such as a manufacturing process. Please note that if you include your name, contact information, or other information that identifies you in the body of your comments, that information will be posted on *http://www.regulations.gov*.
- If you want to submit a comment with confidential information that you do not wish to be made available to the public, submit the comment as a written/paper submission and in the manner detailed (see “Written/Paper Submissions” and “Instructions”).

Written/Paper Submissions

Submit written/paper submissions as follows:

- Mail/Hand delivery/Courier (for written/paper submissions): Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, Rm. 1061, Rockville, MD 20852.
- For written/paper comments submitted to the Division of Dockets Management, FDA will post your comment, as well as any attachments, except for information submitted, marked and identified, as confidential, if submitted as detailed in “Instructions.”

Instructions: All submissions received must include the Docket No. FDA-2014-N-1286 for “Moving Forward: Collaborative Approaches to Medical Device Cybersecurity.” Received comments will be placed in the docket and, except for those submitted as “Confidential Submissions,” publicly viewable at *http://www.regulations.gov* or at the Division of Dockets Management between 9 a.m. and 4 p.m., Monday through Friday.

- Confidential Submissions—To submit a comment with confidential information that you do not wish to be made publicly available, submit your comments only as a written/paper submission. You should submit two copies total. One copy will include the information you claim to be confidential with a heading or cover note that states “THIS DOCUMENT CONTAINS CONFIDENTIAL INFORMATION”. The Agency will review this copy, including the claimed confidential information, in its consideration of comments. The second copy, which will have the claimed confidential information redacted/blacked out, will be available for public viewing and posted on *http://www.regulations.gov*. Submit both copies to the Division of Dockets Management. If you do not wish your name and contact information to be made publicly available, you can provide this information on the cover sheet and not in the body of your comments and you must identify this information as "confidential." Any information marked as "confidential" will not be disclosed except in accordance with 21 CFR 10.20 and other applicable disclosure law. For more information about FDA's posting of comments to public dockets, see 80 FR 56469, September 18, 2015, or access the information at: *http://www.fda.gov/regulatoryinformation/dockets/default.htm*.

Docket: For access to the docket to read background documents or the electronic and written/paper comments received, go to *http://www.regulations.gov* and insert the docket number, found in brackets in the heading of this document, into the "Search" box and follow the prompts and/or go to the Division of Dockets Management, 5630 Fishers Lane, Rm. 1061, Rockville, MD 20852.

Contact Person: Suzanne Schwartz, Suzanne Schwartz, Food and Drug Administration, Center for Devices and Radiological Health, 10903 New Hampshire Ave., Bldg. 66, Rm. 5428, Silver Spring, MD 20993, 301-796-6937, *Suzanne.Schwartz@fda.hhs.gov*.

I. Background

Effective medical device cybersecurity to assure device safety and functionality has become more important with the increasing use of wireless, Internet- and network-connected devices, and the frequent electronic exchange of medical device-related health information. As medical devices become more connected and interoperable, the potential for exploit of device vulnerabilities, whether intentional or not, increases. Rather than impacting a single device or single system, multiple devices or an entire hospital network may be compromised. In the past, the Healthcare and Public Health (HPH) sector has been the target of many attempts at intrusion. Protecting the HPH critical infrastructure from attack by strengthening cybersecurity is a high priority for the Federal government. Cybersecurity is the subject of recent Executive Orders focused on enhancing the cybersecurity of critical infrastructure (E.O. 13636) (Ref. 1) and increasing cybersecurity information sharing (E.O. 13691) (Ref. 2). Furthermore, Presidential Policy Directive 21 tasks the Federal government to work together with the private sector in order to strengthen the security and resilience of critical infrastructure against physical and cyber threats (Ref. 3). This public workshop will bring together diverse stakeholders from the public and private sector to discuss the current state of medical device cybersecurity, including its evolution over the past 12 months. Moreover, the workshop plans to provide a vision for the desired state of medical device cybersecurity through ongoing collaboration and new partnerships over the next 12 months. Meeting participants are encouraged to formulate strategies and feasible action plans to address gaps, such as management of vulnerabilities in legacy devices. These diverse stakeholders include, but are not limited to: Medical device manufacturers; healthcare facilities and personnel (*e.g.*, healthcare providers, biomedical engineers, IT system administrators); professional and trade organizations including medical device cybersecurity consortia; patient groups; insurance providers; cybersecurity researchers; local, State, and Federal Governments; and information security firms.

A voluntary, risk-based framework for achieving enhanced cybersecurity was developed by the National Institute of Standards and Technology (NIST) in collaboration with external public and private sector partners (Ref. 4). Since its release in February 2014, the "Framework for Improving Critical Infrastructure Cybersecurity" (Framework) has been leveraged by entities within the HPH sector to better manage and reduce cybersecurity risks. This workshop aims to highlight some of the ways that the Framework has been employed to better understand, manage, communicate, and mitigate medical device cybersecurity risks across the medical device total product lifecycle.

Medical device cybersecurity vulnerabilities, if exploited, may result in device malfunction, disruption of healthcare services including treatment interventions, inappropriate access to patient information, or compromised electronic health record data integrity. Such outcomes could have a profound impact on patient care and safety. In the last few years, HPH sector stakeholders have been engaged in many collaborative activities that seek to strengthen medical device cybersecurity and, therefore, enhance patient safety. FDA has contributed to these efforts through guidance, multi-stakeholder engagement, outreach, and by hosting a 2014 public workshop on cybersecurity (Ref. 5). The 2016 public workshop announced in this Federal Register notice will build upon previous work by featuring some of the collaborative efforts that address medical device cybersecurity through education and training, information sharing, standards, risk assessment, and tools development.

Though progress is evident, key hurdles continue to impede maturation of the HPH community's cybersecurity posture. This workshop seeks to increase awareness among stakeholders and create a common understanding of potential threats and vulnerabilities, as well as to present proactive preventative measures that may be universally employed as best practices and good cyber hygiene. The workshop also aims to facilitate extensive dialogue and articulate paths forward in the critical areas of information sharing, coordinated vulnerability disclosure and vulnerability management, and the Common Vulnerability Scoring System (CVSS). Information sharing continues to be a challenge as stakeholders work to define processes to create a trusted environment. Coordinated vulnerability disclosure is an important component of information sharing. Proactively identifying, assessing, and managing medical device vulnerabilities before they are exploited is one way to protect against potential patient harm. Vulnerabilities may be identified by the device manufacturer as well as by external entities such as healthcare facilities, cybersecurity researchers, and other sectors of critical infrastructure. As described in

International Organization for Standardization/International Electrotechnical Commission 29147:2014, “Coordinated disclosure, also known as *responsible* disclosure, is a vulnerability disclosure model in which all stakeholders agree to delay publishing vulnerability details for an agreed-upon period of time, generally after a patch to mitigate the vulnerability is available. The model includes steps that simplify the otherwise-complex, back-and-forth communications between the vulnerability finder and the affected manufacturer” (Ref. 6). Coordinated disclosure is just one aspect of vulnerability management. Understanding how a vulnerability may affect device functionality, assessing the vulnerability impact across multiple product types, and identifying mitigations that may be employed until a permanent fix may be implemented are all critical components of vulnerability management that should be addressed throughout the medical device total product lifecycle. This workshop provides an opportunity for stakeholders to explore implementation of coordinated vulnerability disclosure and vulnerability management, including existing standards, models, best practices, and lessons learned in this area.

One of the tools that manufacturers or healthcare facilities may use to assess and manage the impact of vulnerability is CVSS. CVSS is a risk assessment tool that provides an open and standardized method for rating information technology vulnerabilities. However, incorporating CVSS into medical device vulnerability assessments has proven to be a challenge in that it does not directly incorporate patient risk and public health impact factors. This workshop encourages robust dialogue on how CVSS might be adapted for medical devices and how considerations of the use environment might be incorporated in a more standardized manner into medical device CVSS scores.

II. Topics for Discussion at the Public Workshop

The public workshop sessions are designed to incorporate the following general themes:

- Envisioning a roadmap for coordinated vulnerability disclosure and vulnerability management as part of the broader effort to create a trusted environment for information sharing.

○ How might the stakeholder community create incentives to encourage stakeholder participation?

○ What do individual stakeholders need to understand and be aware of regarding coordinated disclosure?

○ What current tools and models presently exist that may aid stakeholders in implementing disclosure and vulnerability management?

○ How can the security researcher community work in collaboration with HPH stakeholders to identify, assess, and mitigate vulnerabilities?

- Sharing FDA's current thinking on the implementation of the Framework in the medical device total product lifecycle.
- Adapting cybersecurity and/or risk assessment tools such as CVSS for the medical device operational environment.
- Adapting and/or implementing existing cybersecurity standards for medical devices.
- Understanding the challenges that manufacturers face as they increase collaboration with external third parties (cybersecurity researchers, Information Sharing and Analysis Organizations (ISAOs), and end users), to resolve cybersecurity vulnerabilities that impact their devices. Note that an ISAO is a group created to gather, analyze, and disseminate critical infrastructure information (Ref. 7).
- Gaining situational awareness of the current activities in the HPH sector to enhance medical device cybersecurity.
- Identifying cybersecurity gaps and challenges that persist in the medical device ecosystem and begin crafting action plans to address them.
- *Registration:* Registration is free and available on a first-come, first-served basis. Persons interested in attending this public workshop must register online by January 13, 2016, at 4 p.m. Early registration is recommended because facilities are limited and, therefore, FDA may limit the number of participants from each organization. If time and space permits, onsite registration on the day of the public workshop will be provided beginning at 8 a.m.

- If you need special accommodations due to a disability, please contact Susan Monahan, Center for Devices and Radiological Health, Office of Communication and Education, 301-796-5661 or email: *susan.monahan@fda.hhs.gov* no later than January 7, 2016.

- Please provide complete contact information for each attendee, including name, title, affiliation, email, and telephone number. Those without Internet access should contact Susan Monahan to register. Registrants will receive confirmation after they have been accepted. You will be notified if you are on a waiting list.

Streaming Webcast of the Public Workshop: This public workshop will also be Webcast. The Webcast link will be available on the registration Web page after January 13, 2016. Please visit FDA's Medical Devices News & Events—Workshops & Conferences calendar at *http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/default.htm*. Select this meeting/public workshop from the posted events list. If you have never attended a Connect Pro event before, test your connection at *https://collaboration.fda.gov/common/help/en/support/meeting_test.htm*. To get a quick overview of the Connect Pro program, visit *http://www.adobe.com/go/connectpro_overview*. FDA has verified the Web site addresses in this document, but FDA is not responsible for any subsequent changes to the Web site after this document publishes in the Federal Register.

Transcripts: Please be advised that as soon as a transcript is available, it will be accessible at *http://www.regulations.gov*. It may be viewed at the Division of Dockets Management (see ADDRESSES). A transcript will also be available in either hardcopy or on CD-ROM, after submission of a Freedom of Information request. The Freedom of Information office address is available on the Agency's Web site at *http://www.fda.gov*. A link to the transcripts will also be available approximately 45 days after the public workshop on the Internet at *http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/default.htm*. (Select this public workshop from the posted events list).

III. References

The following references are on display in the Division of Dockets Management (see ADDRESSES) and are available for viewing by interested persons between 9 a.m. and 4 p.m., Monday through Friday; they are also available electronically at *http://www.regulations.gov*. FDA has verified the Web site addresses, as of the date this document publishes in the Federal Register, but Web sites are subject to change over time.

1. Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," February 19, 2013 (*http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf*).

2. Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing," February 13, 2015 (*http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf*).

3. Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience," February 12, 2013 (*http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil*).

4. National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," version 1, February 12, 2014 (*http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf*).

5. Food and Drug Administration, "Public Workshop—Collaborative Approaches for Medical Device and Healthcare Cybersecurity, October 21-22, 2014." October 11, 2015 (*http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm412979.htm*).

6. "ISO/IEC 29147:2014—Information Technology—Security Techniques—Vulnerability Disclosure," (*http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170*).

7. Department of Homeland Security, "Frequently Asked Questions About Information Sharing and Analysis Organizations (ISAOs)," November 17, 2015 (*http://www.dhs.gov/isao-faq*).

Dated: December 2, 2015.
Peter Lurie Kux,
Associate Commissioner for Public Health Strategy and Analysis

[FR Doc. 2015-30772 Filed 12-4-15; 8:45 am]

BILLING CODE 4164-01-P

Notes Section:

www.fda.gov/medicalcountermeasures